
GFI MailSecurity for Exchange/SMTP 10

Manual

By GFI Software Ltd.



<http://www.gfi.com>
Email: info@gfi.com

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of GFI Software Ltd.

GFI MailSecurity is copyright of GFI SOFTWARE Ltd. © 2000-2008 GFI Software Ltd. All rights reserved.

GFI MailSecurity is a registered trademark and GFI Software Ltd. and the GFI logo are trademarks of GFI Software Ltd. in the Europe, the United States and other countries.

Version 10.0 - Last updated: March 02, 2009

Contents

About GFI MailSecurity	1
Introduction to GFI MailSecurity.....	1
Key features of GFI MailSecurity	1
Virus checking using multiple virus engines	1
Email attachment checking/filtering	1
Trojan and Executable Scanner	2
HTML Sanitizer.....	2
Decompression filter	2
GFI MailSecurity components.....	2
GFI MailSecurity from a user's perspective	3
Add-ons – GFI MailEssentials.....	3
 Installing GFI MailSecurity	 5
Introduction	5
Typical deployment scenarios.....	5
Installing GFI MailSecurity on your mail server.....	5
Installing GFI MailSecurity on a mail relay server	6
Installing GFI MailSecurity in front of your firewall	7
Installing GFI MailSecurity on an Active/Passive Cluster	7
Installing GFI MailSecurity on an Active/Active Cluster	9
Which installation mode should I use?.....	9
Active Directory mode	9
SMTP mode	9
System requirements	10
Hardware requirements	10
Preparing to install GFI MailSecurity on an IIS mail relay server	11
Step 1: Verify installation of IIS SMTP and WWW services	11
Step 2: Specify mail relay server name and assign an IP	11
Step 3: Configure the SMTP service to relay mail to your mail server	12
Step 4: Secure your mail relay server	14
Step 5: Configure your mail server to relay email via the Gateway server	16
Step 6: The MX record of your domain must point to the mail relay server.....	17
Step 7: Test your new mail relay server.....	18
Step 8: Install GFI MailSecurity on the mail relay server	18
Preparing to install GFI MailSecurity on your mail server.....	18
Installing GFI MailSecurity	18
GFI MailSecurity Post-Installation Wizard.....	23
Adding GFI MailSecurity to the Windows DEP Exception List.....	26
Securing access to the GFI MailSecurity configuration/quarantine	27
Adding local host to the trusted sites list.....	30
Securing access to the GFI MailSecurity Quarantine RSS feeds.....	31
Accessing the GFI MailSecurity Configuration and Quarantine Store	33
Accessing the configuration from the GFI MailSecurity machine	33
Accessing the configuration from a remote machine	34
Entering your license key after installation	35
Upgrading from GFI MailSecurity 8 to GFI MailSecurity 10.....	36
Upgrading from GFI MailSecurity 9 to GFI MailSecurity 10.....	38

Quarantine Upgrade tool.....	39
Using the quarantine upgrade tool	39
General settings	41
Introduction to settings	41
Define the administrator's email address	41
Configuring proxy server settings for automatic updates.....	42
Adding Local Domains	43
SMTP server bindings.....	43
Managing local users in SMTP mode	44
To add a new local user follow these steps:	45
To remove a local user follow these steps:	46
Configuring virus checking	47
Configuring Virus Scanning Engines	47
AVG configuration	48
AVG web site.....	50
Kaspersky configuration.....	50
Kaspersky web site	51
BitDefender configuration	52
BitDefender website	53
McAfee configuration	53
McAfee website	54
Norman configuration.....	54
Norman website	55
Virus scanner actions.....	56
Virus scanner updates	57
Triggering the virus update manually	58
Setting the Virus Scanning Engines scan priority	58
Configuring Virus Scanning optimizations	58
Configuring Information Store Scanning.....	59
Configuring Attachment Checking	63
Introduction to Attachment Checking	63
Creating an Attachment Checking rule	63
Removing attachment rules	68
Make changes to an existing rule	69
Enabling/disabling rules	69
Changing the rule priority	69
Configuring Content Checking	71
Introduction to Content Checking.....	71
Creating a Content Checking rule	71
Remove content checking rules.....	77
Make changes to an existing content checking rule	78
Enabling/disabling rules	78
Changing the rule priority	78
Decompression engine	79
Introduction to the Decompression engine	79
Configuring the decompression engine filters.....	80
Check password protected archives	80
Check corrupted archives	80
Check for recursive archives.....	81
Check size of uncompressed files in archives	82
Check for amount of files in archives	83
Scan within archives	83

Configuring decompression filter actions	84
Enable/disable decompression filters	85
The Trojan & Executable Scanner	87
Introduction to the Trojan & Executable Scanner	87
What is a Trojan horse?	87
Difference between Trojans and viruses.....	87
How does the Trojan & Executable Scanner work?.....	87
Configuring the Trojan & Executable Scanner.....	88
Configuring the security level	88
Configuring actions	89
Trojan & Executable Scanner updates	89
Triggering the Trojan & Executable Scanner update manually	90
The Email Exploit Engine	91
Introduction to e-mail exploits	91
What is an exploit?	91
What is an e-mail exploit?	91
Difference between Anti-Virus software & Email Exploit Detection software	91
Configuring the Email Exploit Engine.....	91
Enable/Disable email exploits	91
Configuring the Email Exploit Engine properties.....	92
Email Exploit Engine updates	94
Triggering the Email Exploit Engine update manually	94
The HTML Sanitizer	95
Introduction to the HTML Sanitizer	95
Why remove HTML scripts?.....	95
Configuring the HTML Sanitizer.....	95
Patch Checking	97
Introduction to Patch Checking	97
Downloading and installing software patches	97
Quarantine	99
Introduction to the Quarantine Store	99
The Quarantine Store.....	99
Searching for emails in the Quarantine Store	100
Search Folders.....	101
What is a search folder?	101
Why are search folders useful?.....	101
Grouping quarantined emails in Search Folders.....	101
Changing Search Folder properties	105
Deleting Search Folders.....	105
Approving emails from the Quarantine Store.....	105
Deleting emails from the Quarantine Store.....	106
Rescanning emails from the Quarantine Store.....	107
View the full security threat report of an email.....	108
Enable email approval via HTML approval forms	110
How to approve or delete quarantined emails from an email client	111
Quarantined mail from the user point of view	111
Enable quarantine RSS feeds.....	112
What is RSS?	112
How does GFI MailSecurity use RSS?	112
How do I configure RSS on a quarantine folder?.....	113

How do I subscribe to a quarantine search folder RSS feed?	114
Enable the Directory Harvesting filter on quarantined emails.....	115
Reporting	119
Introduction to GFI MailSecurity Reporting.....	119
Configuring the statistical information database	119
Configuring a Microsoft Access database backend	120
Configuring a Microsoft SQL Server database backend.....	121
Creating a new database on Microsoft SQL Server.....	122
Realtime Monitor	125
About the Realtime Monitor	125
Monitoring email activity.....	125
Miscellaneous	127
Version Information	127
Additional Copyright Information	127
Libxml2: The MIT License	127
Advanced topics	129
Customizing the notification templates	129
Variables used in XSL-based notification templates.....	130
Notify user and notify manager notifications (in notifyuser folder and notifymanager folder respectively)	130
Setting Virus Scanning API Performance Monitor Counters	132
Troubleshooting	135
Introduction	135
Knowledge Base	135
Web Forum	135
Request technical support	135
Build notifications	136
GFI MailSecurity ReportPack - Introduction	137
About GFI ReportCenter	137
About the GFI MailSecurity 10.0 ReportPack	138
Components of the GFI MailSecurity 10.0 ReportPack	138
GFI ReportCenter framework.....	138
GFI MailSecurity 10.0 default reports	140
Report scheduling service.....	140
Key features	140
Centralized reporting.....	140
Default reports.....	140
Distribution of reports via email.....	140
Report export to various formats.....	141
Printing	141
Report scheduling	141
Report customization	141
Favorites.....	141
Wizard assisted configuration	141
License scheme and evaluation period	141
Evaluation period	141
Purchasing a license key	141
GFI MailSecurity ReportPack - Installation	143

System requirements	143
Installation procedure	143
Launching GFI MailSecurity 10.0 ReportPack for GFI ReportCenter	147
Selecting a product	147
GFI MailSecurity ReportPack - Default reports	149
Introduction	149
Generating a default report	150
Example: Generating a “Monthly email traffic” report based on the last 12 months data	150
Viewing the generated report	151
Report browsing options	152
Report storage and distribution options	152
Adding default reports to the list of favorite reports	152
GFI MailSecurity ReportPack - Custom reports	153
Introduction	153
Creating a new custom report	153
Generate a custom report	155
Editing a custom report	156
Deleting a custom report	156
Adding custom reports to the list of favorite reports	156
GFI MailSecurity ReportPack - Scheduling reports	157
Introduction	157
Scheduling a report	157
Viewing the list of scheduled reports	162
Viewing the scheduled reports activity	162
Enable/disable a scheduled report	163
Editing a scheduled report	164
Deleting a scheduled report	164
GFI MailSecurity ReportPack - Configuring default options	165
Introduction	165
Which GFI MailSecurity reporting database is being used?	165
Configuring the GFI MailSecurity reporting database source	166
Configuring default scheduling options	167
GFI MailSecurity ReportPack - General options	169
Entering your license key after installation	169
Viewing the current licensing details	170
Viewing the GFI MailSecurity 10.0 ReportPack version details	170
Checking the web for newer builds	170
GFI MailSecurity ReportPack - Exporting Settings	173
Introduction	173
Exporting the GFI MailSecurity 10.0 ReportPack Settings	173
Importing the GFI MailSecurity 10.0 ReportPack Settings	175
GFI MailSecurity ReportPack - Default Reports List	177
Executive Reports	177
Viruses Blocked Monthly	177
Inbound and outbound email traffic per week days	178
Inbound email traffic per week days	178
Outbound email traffic per week days	179

Monthly email traffic	180
Processed and blocked emails per month	181
Processed emails per month.....	182
Blocked emails per month.....	183
Administrative Reports	184
Processed and blocked emails per four hours.....	184
Processed emails per four hours	185
Blocked emails per four hours.....	186
Daily processed and blocked emails.....	187
Processed and blocked emails per week.....	188
Monthly processed and blocked emails	189

GFI MailSecurity ReportPack - Troubleshooting 191

Introduction	191
Knowledge Base	191
Web Forum	191
Request technical support	191
Build notifications	192

About GFI MailSecurity

Introduction to GFI MailSecurity

The need to monitor email messages for dangerous, offensive or confidential content has never been more evident. The most deadly viruses, able to cripple your email system and corporate network in minutes, are being distributed worldwide via email in a matter of hours (for example, the MyDoom worm). Products that perform single vendor anti-virus scanning do not provide sufficient protection. Worse still, email is likely to become the means for installing backdoors (Trojans) and other harmful programs to help potential intruders break into your network. Products restricted to a single anti-virus engine will not protect against email exploits and attacks of this kind.

Your only defense is to install a comprehensive email content checking and anti-virus solution to safeguard your mail server and network. GFI MailSecurity acts as an email firewall and protects you from email viruses, exploits and threats, as well as email attacks targeted at your organization.

GFI MailSecurity is totally transparent to your users and does not require additional user training.

Key features of GFI MailSecurity

Virus checking using multiple virus engines

GFI MailSecurity scans email for viruses using multiple anti-virus engines. Scanning email at the gateway and at mail server level prevents viruses from entering and/or spreading within your network. Furthermore, you can avoid the embarrassment of sending infected emails to customers as GFI MailSecurity also checks outgoing mail for viruses. GFI MailSecurity includes the industrial strength Norman and BitDefender anti-virus engines that have received various awards. You also have the option to add the AVG, McAfee and Kaspersky anti-virus engines. Multiple anti-virus engines give you a higher level of security since anti-virus engines complement each other and lower the average response time to a virus outbreak. GFI MailSecurity also includes an auto-update facility that allows you to configure the anti-virus engines so that they automatically check and download any available updates without administrator intervention.

Email attachment checking/filtering

GFI MailSecurity's key feature is the ability to check all inbound and outbound email. It can quarantine all email with dangerous attachments, such as *.exe, *.vbs and other files. Such attachments are more likely to carry a virus, worm or email attack. Since email

viruses can spread so quickly and cause immense damage, it is best to quarantine such emails before they are distributed to your email users. When GFI MailSecurity quarantines an email, the administrator can review it and then delete or approve the message.

Furthermore, you might choose to quarantine mails carrying *.mp3 or *.mpg files, as these hog bandwidth and can needlessly burden a mail server's disk space.

The Attachment Checking module has effectively saved thousands of companies from the LoveLetter virus.

Trojan and Executable Scanner

GFI MailSecurity is able to analyze incoming executables and rate the risk-level of an executable through a GFI patented process. Through the Trojan and Executable Scanner, GFI MailSecurity can detect and block potentially dangerous and unknown Trojans before they enter your network.

HTML Sanitizer

The advent of HTML email has made it possible for hackers/virus writers to trigger commands by embedding them in HTML mail. GFI MailSecurity scans the email body parts and any .htm/.html attachments for scripting code, and cleans up the HTML by removing all the scripting code. The HTML Sanitizer thus protects you from potentially malicious HTML email, containing HTML viruses and attacks launched via HTML email.

Decompression filter

The decompression filter is used to decompress and analyze compressed files (archives) attached to emails. This filter is able to check for and block password-protected archives, corrupted archives and recursive archives. Furthermore, this engine can also monitor the size and amount of the files included in an archive. You can configure this filter to quarantine or delete archives that exceed the specified file count or file size.

GFI MailSecurity components

GFI MailSecurity scan engine

The GFI MailSecurity scan engine analyzes the content of all inbound and outbound email. If you install GFI MailSecurity on the Microsoft Exchange machine, it will also scan the information store. If installed on a Microsoft Exchange 2007 machine, GFI MailSecurity will scan the information store only if the Mailbox Server Role is installed. If you install GFI MailSecurity on a Microsoft Exchange 2007 machine with the Hub Transport Server Role, it will also analyze internal email. When GFI MailSecurity quarantines an email, it informs the appropriate supervisor/administrator via Email/RSS feed, depending on the options you configure.

GFI MailSecurity configuration

Through the GFI MailSecurity configuration, you can configure GFI MailSecurity to fit your needs.



Screenshot 1 - GFI MailSecurity Configuration

GFI MailSecurity from a user's perspective

GFI MailSecurity is totally transparent to the user. This means that the user will not notice that GFI MailSecurity is active until it blocks an email that triggers a rule, for example, an email that contains a forbidden attachment or a virus.

In the case of a suspicious attachment, GFI MailSecurity will quarantine the email for review by the administrator. Optionally, the recipient will receive a message indicating that the mail is awaiting administrator review. As soon as the administrator approves the email, GFI MailSecurity will forward the email to the recipient.

Add-ons – GFI MailEssentials

A companion product to GFI MailSecurity is GFI MailEssentials. GFI MailEssentials adds a number of corporate email features to your mail server, notably:

- Anti-spam, using a variety of methods including Bayesian analysis
- Email management, including disclaimers, POP3 downloader and server-based auto replies and more.

For more information, please visit the GFI website at <http://www.gfi.com>.

NOTE: GFI MailEssentials is available at a bundle price if purchased in combination with GFI MailSecurity.

Installing GFI MailSecurity

Introduction

This chapter explains how to install and configure GFI MailSecurity. You can install GFI MailSecurity directly on your mail server or you can choose to install it on a separate machine configured as a mail relay/gateway server. When installing on a separate machine, you must first configure the machine to relay the inbound and outbound emails to your mail server prior to installing this mail security software.

In order to function correctly, GFI MailSecurity requires access to the complete list of all your email users and their email addresses. This is required in order to configure content policy rules such as attachment checking and content checking. GFI MailSecurity can access the list of email users in two ways: either by querying your Active Directory (requires installing this software in **Active Directory mode**) or by importing the list from your SMTP Server (requires installing this software in **SMTP mode**). The mode to be used depends entirely on your network setup and the machine on which you will be installing this mail security software. You can choose the required access mode during the installation of GFI MailSecurity.

Typical deployment scenarios

Installing GFI MailSecurity on your mail server

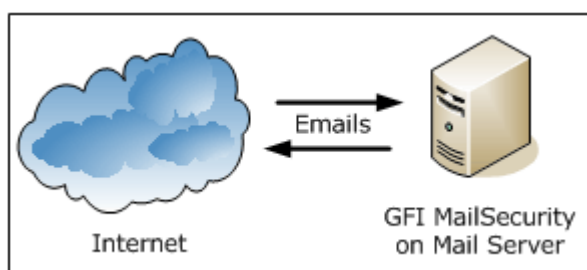


Figure 1 - Installing GFI MailSecurity on your mail server

You can install GFI MailSecurity directly on your mail server, without any additional configuration required. Moreover you can also choose any of the two installation modes (i.e., Active Directory mode or SMTP mode) to define how GFI MailSecurity will retrieve the list of email users since your mail server will have access to both the Active Directory as well as to the list of SMTP users which is contained on the mail server itself.

NOTE: GFI MailSecurity can be only installed in the following Microsoft Exchange 2007 installations:

- Edge Server Role
- Hub Transport Role (and any other Microsoft Exchange 2007 server roles which are irrelevant to GFI MailSecurity)
- Mailbox and Hub Transport Server Role (and any other Microsoft Exchange 2007 server roles which are irrelevant to GFI MailSecurity)

Installing GFI MailSecurity on a mail relay server

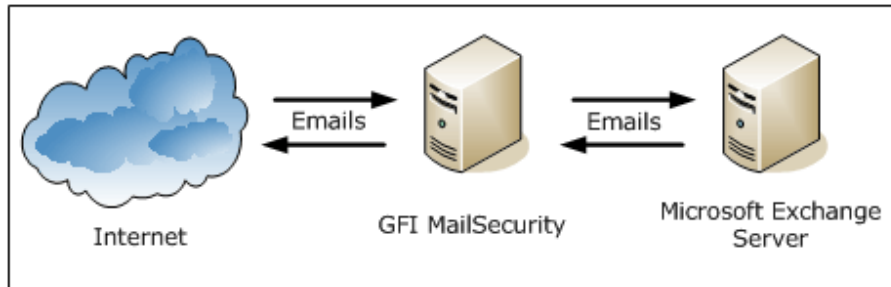


Figure 2 - Installing GFI MailSecurity on a mail gateway/relay server

When installing on a separate server (i.e., on a server which is not your mail server), you must first configure that machine to act as a gateway (also known as “Smart host” or “Mail relay” server) for all your email. This means that all inbound email must pass through this machine for scanning before being relayed to the mail server for distribution (i.e., it must be the first to receive all emails destined for your mail server). The same applies for outbound emails: The mail server must relay all outgoing emails to the gateway machine for scanning before they are conveyed to the external recipients via Internet (i.e. it must be the last 'stop' for emails destined for the Internet). In this way, GFI MailSecurity checks all your inbound and outbound mail before this is delivered to the recipients.

NOTE 1: You must install GFI MailSecurity in SMTP Gateway mode if you are running Lotus Notes or another SMTP/POP3 server.

NOTE 2: If you are running a Windows NT network, the machine running GFI MailSecurity can be separate from your Windows NT network – GFI MailSecurity does not require Active Directory when installed in SMTP mode.

Installing GFI MailSecurity in front of your firewall

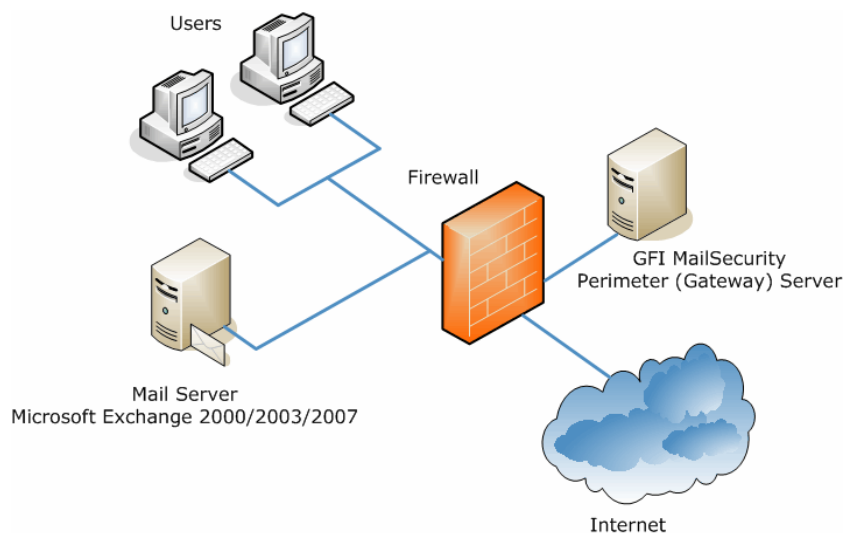


Figure 3 - Installing GFI MailSecurity on a separate machine on a DMZ

If running a Windows 2000/2003 firewall such as Microsoft ISA Server, a good way to deploy GFI MailSecurity is to install it on a separate machine in front of your firewall or on the firewall itself. This allows you to keep your corporate mail server behind the firewall. GFI MailSecurity will act as a smart host/mail relay server when installed on the perimeter network (also known as DMZ - demilitarized zone).

NOTE: In a Microsoft Exchange Server 2007 environment, the mail relay server in the DMZ can be a machine running Microsoft Exchange Server 2007 with the Edge Transport Server Role installed.

When GFI MailSecurity is not installed on your mail server:

- You can perform maintenance on your mail server whilst still receiving email from the Internet.
- Fewer resources are used on your mail server.
- Additional fault tolerance – if anything happens to your mail server, you can still receive email. This email is then queued on the GFI MailSecurity machine.

NOTE: GFI MailSecurity does not require a dedicated machine when not installed on the mail server. For example, you can install GFI MailSecurity on your firewall (i.e. on your ISA Server) or on machines running other applications such as GFI MailEssentials.

Installing GFI MailSecurity on an Active/Passive Cluster

NOTE: Installing GFI MailSecurity on a Microsoft Exchange Server 2007 cluster environment is currently not supported.

To install GFI MailSecurity on an Active/Passive cluster you must install GFI MailSecurity on each node.

NOTE: Although you can install GFI MailSecurity on an Active/Passive cluster, bear in mind that you still need to configure and manage a GFI MailSecurity installation per node. The configuration settings and quarantine emails are not shared between nodes.

On each node, you have to do the following:

- Install GFI MailSecurity on the node local hard drive.
NOTE: Do not install GFI MailSecurity on the shared drive.
- Install the GFI MailSecurity WWW virtual directory on the node's **Default Web Site**.
- If you are installing on an IIS cluster, make sure you bind GFI MailSecurity to the **Clustered** SMTP Virtual Server instance.

The following steps show you how to install GFI MailSecurity in a typical Active/Passive Cluster environment. For this scenario, assume the cluster, named **MAILCLUSTER**, is made up of two nodes, named **Node1** and **Node2**.

1. Using the **Cluster Administrator** console make **Node1** active.
2. Install GFI MailSecurity on the local hard drive of **Node2** as described in the 'Installing GFI MailSecurity' section of this chapter. When you reach the **IIS Setup** step of the installation, select **Default Web Site** to host the GFI MailSecurity WWW virtual directory.

NOTE: The **Default Web Site** IP address of **Node2** should not be set to 'All unassigned'. You should configure the **Default Web Site** to use the IP address of the **MAILCLUSTER** machine.

3. When the GFI MailSecurity installation on **Node2** completes, you should be able to access the **Node2** configuration using the following URL: <http://Node2/MailSecurity/>

4. From the **Cluster Administrator** console, make **Node2** active.

5. Install GFI MailSecurity on the local hard disk of **Node1** as described in the 'Installing GFI MailSecurity' section of this chapter. When you reach the **IIS Setup** step of the installation, select **Default Web Site** to host the GFI MailSecurity WWW virtual directory.

NOTE: The **Default Web Site** IP address of **Node1** should not be set to 'All unassigned'. You should configure the **Default Web Site** to use the IP address of the **MAILCLUSTER** machine.

6. When the GFI MailSecurity installation on **Node1** completes, you should be able to access the **Node1** configuration using the following URL: <http://Node1/MailSecurity/>

7. To access the product configuration of the currently active node use the following URL: <http://MAILCLUSTER/MailSecurity/>.

NOTE 1: To access product configuration from a remote machine you must configure the **GFI MailSecurity SwitchBoard** application, making sure that the **MAILCLUSTER** name/IP is specified for **IIS Mode**. For more information, refer to the 'Securing access to the GFI MailSecurity configuration/quarantine' section in this chapter.

NOTE 2: You will only be able to access the URL <http://MAILCLUSTER/MailSecurity/> if you assign the IP address of the **MAILCLUSTER** machine to the **Default Web Site** for **Node1** and **Node2** during the **IIS Setup** installation step.

8. The installation of GFI MailSecurity on an Active/Passive cluster is now complete.

NOTE: If Service Pack 2 for Microsoft Exchange Server 2003 is not installed on a Microsoft Exchange Server 2003 cluster installation, Internet Information Services Web sites that are hosted on the cluster will not start automatically when an Exchange Server 2003 virtual

server fails over to a cluster node. More information about this issue can be found in [Microsoft Knowledge Base Article 885440](#).

Due to the above, the GFI MailSecurity configuration could become unavailable following a failover or moving of an Exchange Virtual Server from one node of the cluster to the other.

Installing Service Pack 2 for Exchange Server 2003 is thus recommended. Guidelines on how to install Exchange Server 2003 service packs in a clustered Exchange Server environment can be found in [Microsoft Knowledge Base Article 867624](#).

To uninstall GFI MailSecurity from the **MAILCLUSTER** cluster environment outlined above, follow these steps:

1. Using the **Cluster Administrator** console make **Node1** active.
2. Uninstall GFI MailSecurity from **Node2**.
3. Using the **Cluster Administrator** console make **Node2** active.
4. Uninstall GFI MailSecurity from **Node1**.
5. The uninstallation of GFI MailSecurity on an Active/Passive cluster is now complete.

Installing GFI MailSecurity on an Active/Active Cluster

Installing GFI MailSecurity on an Active/Active cluster is currently not supported.

Which installation mode should I use?

Active Directory mode

When installed in Active Directory mode, GFI MailSecurity creates user-based rules, such as Attachment Checking and Content Checking rules, based on the list of users available in Active Directory. This means that the machine running GFI MailSecurity must be behind your firewall and must have access to the Active Directory containing all your email users (i.e., the machine must be part of the Active Directory domain). You can install GFI MailSecurity in Active Directory mode directly on your mail server as well as on any other domain machine that is configured as a mail relay server in your domain.

SMTP mode

In SMTP mode, GFI MailSecurity will create user-based rules, such as Attachment Checking and Content Checking rules, based on the list of email users/addresses available on your mail server. This means that you must install GFI MailSecurity in SMTP mode if your machine does not have access to the Active Directory containing all your email users. This includes machines that are not part of your Active Directory domain (i.e., non-domain machines) as well as machines in a DMZ. However, you can still install GFI MailSecurity in SMTP mode on your mail server as well as on any other machine that has access to Active Directory containing all (email) users.

NOTE: Both installation modes have the same scanning features and performance. The only difference between Active Directory and SMTP

installation mode is the way that GFI MailSecurity accesses/gathers the list of email users for generating its scanning rules and notifications.

System requirements

To install GFI MailSecurity you need:

- Windows Server 2008/2003 (x32 or x64 Edition) or Windows 2000 Professional/Server/Advanced Server (Service Pack 1 or higher) or Windows XP

NOTE: Since the version of Internet Information Services (IIS) included in Windows XP is limited to serving only 10 simultaneous client connections, installing GFI MailSecurity on a machine running Windows XP could affect its performance.

- Microsoft Exchange Server 2007, 2003, 2000 (SP1), 5.5, 5, 4, or Lotus Notes 4.5 and up, or any SMTP/POP3 mail server

NOTE 1: If you are installing on Microsoft Exchange Server 2007, you need to have either an Edge Server Role, Hub Transport Role or Mailbox Server Role and Hub Transport Server Role installed. GFI MailSecurity cannot be installed on a Microsoft Exchange 2007 machine with only Mailbox Server Role installed.

NOTE 2: When using Small Business Server, ensure you have installed Service Pack 2 for Exchange Server 2000 and Service Pack 1 for Exchange Server 2003.

- Microsoft .Net framework 2.0
- MSMQ – Microsoft Messaging Queuing Service
- Internet Information Services (IIS) (x32 or x64 Edition) – SMTP service and World Wide Web service

NOTE: If installing on a Microsoft Exchange 2007 machine, the IIS SMTP service is not required, since it has its own built in SMTP server.

- Microsoft Data Access Components (MDAC) 2.8

IMPORTANT: Disable anti-virus software from scanning the GFI MailSecurity directories. Anti-virus products are known to both interfere with normal operation as well as slow down any software that requires file access. In fact, Microsoft does not recommend running file-based anti-virus software on the mail server. For more information, please refer to <http://kbase.gfi.com/showarticle.asp?id=KBID001559>.

IMPORTANT: GFI MailSecurity directories should never be backed up using backup software.

Hardware requirements

The hardware requirements for GFI MailSecurity are:

- Pentium 4 (or equivalent) - 2Ghz
- 512MB RAM
- 1.5 GB of physical disk space

Preparing to install GFI MailSecurity on an IIS mail relay server

In order to install GFI MailSecurity on a mail relay/gateway machine, it must be running the IIS SMTP Service and World Wide Web service. You must also configure the machine as an SMTP relay to your mail server. This means that the MX record of your domain must be pointing to the gateway machine. This section describes how you can configure your mail relay and install GFI MailSecurity.

About Windows 2000/2003 IIS SMTP & World Wide Web services

The SMTP service is part of IIS, which is part of Windows 2000/2003/XP. It is used as the message transfer agent of Microsoft Exchange Server 2000/2003, and has been designed to handle large amounts of mail traffic.

The World Wide Web service is also part of IIS. It uses the HTTP protocol to handle web client requests on a TCP/IP network.

The IIS SMTP service and World Wide Web service are included in every Windows 2000/2003/XP distribution.

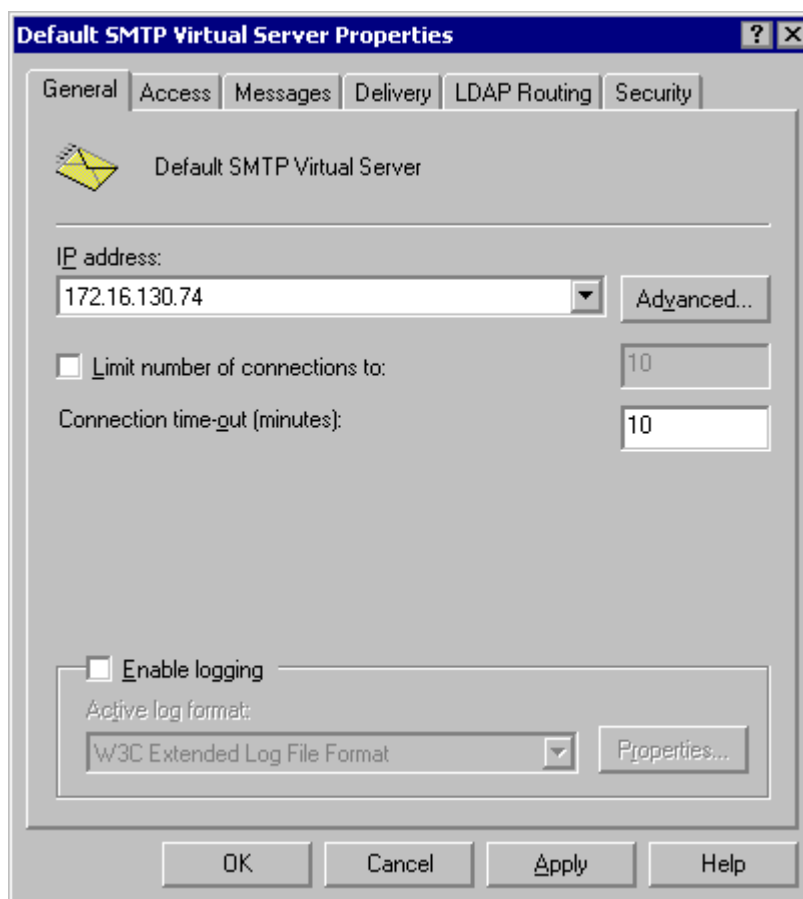
Step 1: Verify installation of IIS SMTP and WWW services

GFI MailSecurity uses the Windows 2000/2003/XP IIS SMTP service as its SMTP server.

1. On the taskbar, click **Start ► Settings ► Control Panel**. Double-click **Add/Remove Programs** and then click **Add/Remove Windows Components**.
2. From the dialog on display, locate and click the **Internet Information Services (IIS) component**, then click **Details**.
3. Select the **SMTP Service** check box and **World Wide Web Service** check box. Click **OK** to start the installation of the selected services. Follow the onscreen instructions and wait until the installation completes.

Step 2: Specify mail relay server name and assign an IP

1. On the taskbar, click **Start ► Settings ► Control Panel**. Double-click **Administrative Tools** and then double-click **Internet Information Services**.
2. Expand the server name node, right-click the **Default SMTP Virtual Server** node and then click **Properties**.



Screenshot 2 - Assign an IP address to the mail relay server

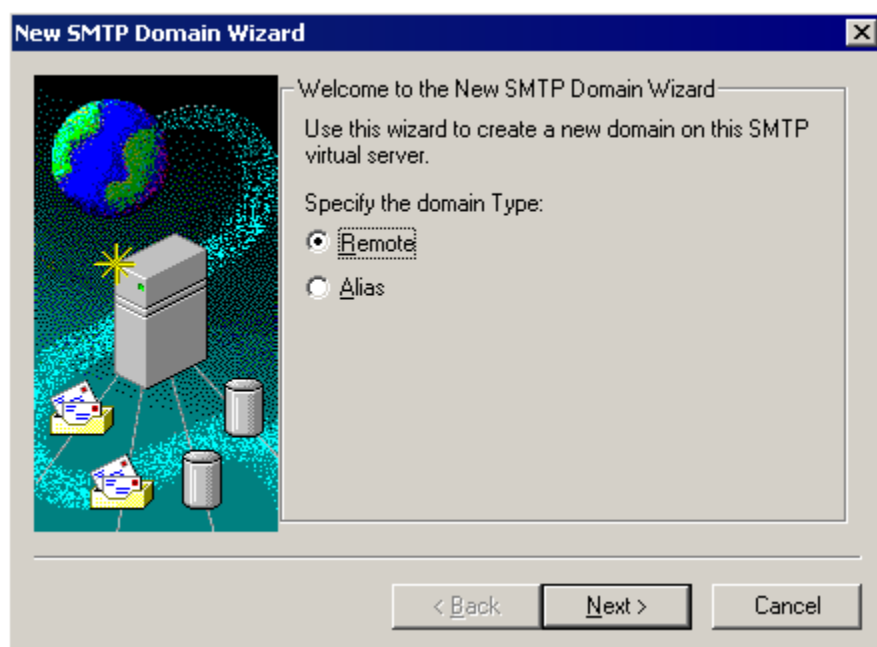
3. Assign an IP address to the SMTP relay server from the **IP address** list and then click **OK**.

Step 3: Configure the SMTP service to relay mail to your mail server

Now you must configure the SMTP service to relay inbound messages to your mail server.

Start by creating a local domain in IIS to route mail:

1. On the taskbar, click **Start ► Settings ► Control Panel**. Double-click **Administrative Tools** and then double-click **Internet Information Services**.
2. Expand the server name node then expand the **Default SMTP Virtual Server** and then click **Domains**. By default, you should have a **Local (Default)** domain with the fully qualified domain name of the server.
3. Configure the domain for inbound message relaying as follows:
 - a) Right-click the **Domains** node, and then click **New ► Domain**.



Screenshot 3 - SMTP Domain Wizard - Selecting domain type

- b) Select **Remote** and then click **Next**.
- c) Type the domain name in the **Name** box and then click **Finish**.

IMPORTANT NOTE ABOUT LOCAL DOMAINS

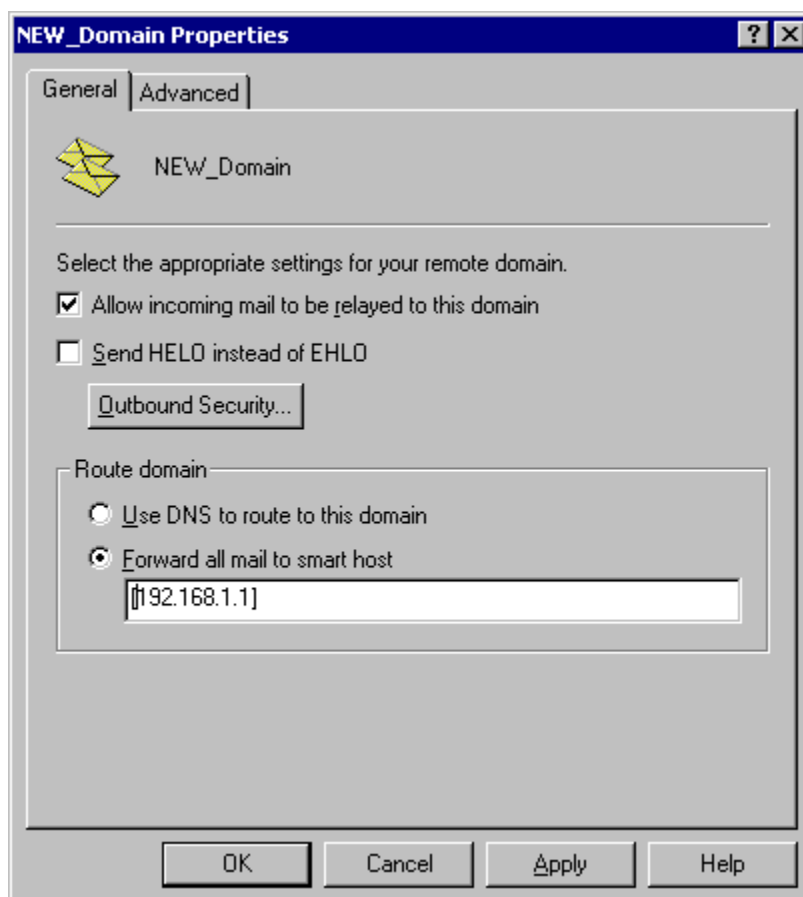
NOTE: Upon installation, GFI MailSecurity will import Local Domains from the IIS SMTP service. If you add additional Local Domains in IIS SMTP service, you must also add these domains to GFI MailSecurity because this does not detect newly added Local Domains automatically. You can add more/new Local Domains using the GFI MailSecurity configuration. For more information, refer to the 'Adding local domains' section in the General Settings chapter of this manual.

Configure the domain to relay email to your mail server:

1. Right-click the domain you just created and then click **Properties**. Select the **Allow the Incoming Mail to be relayed to this domain** check box.
2. In the Route domain dialog box, click **Forward all email to smart host** and type the IP address (in square brackets) of the server which will handle the emails addressed to this new domain. For example, [123.123.123.123]

NOTE: The square brackets are used to differentiate an IP address from a hostname (which does not require square brackets), i.e., the server detects an IP address from the square brackets.

3. Click **OK**.

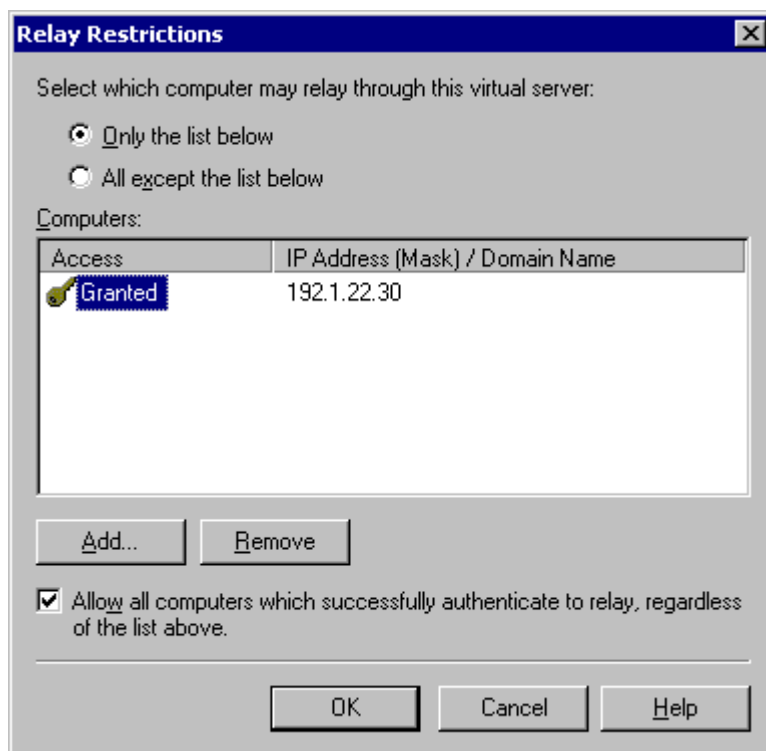


Screenshot 4 - Configure the new domain

Step 4: Secure your mail relay server

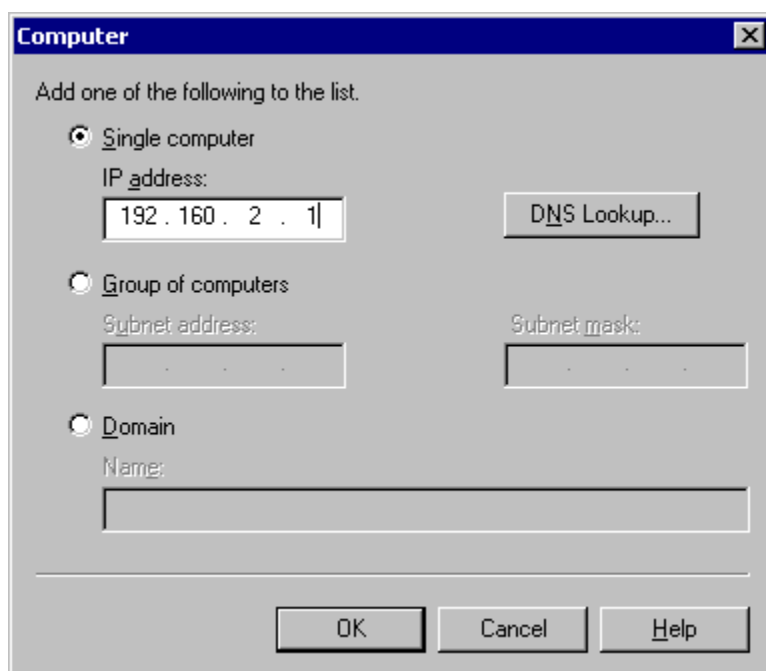
In this step, you will set up your SMTP virtual server's mail Relay Restrictions. This means that you must specify which machines may relay email through this virtual server (i.e., effectively limit the servers that can send email via this server).

1. Right-click the **Default SMTP Virtual Server** node and then click **Properties**.
2. In the properties dialog box, click the **Access** tab and then click **Relay** to open the **Relay Restrictions** dialog box.



Screenshot 5 - Relay Restrictions dialog

3. Click **Only the list below** and then click **Add** to specify the list of permitted computers.



Screenshot 6 - Specify machines which may relay email via virtual server

4. In the **Computer** dialog box, specify the IP of the mail server that will be forwarding the email to this virtual server and then click **OK** to add the entry to the list.

NOTE: You can specify the IP of a single computer, group of computers or a domain:

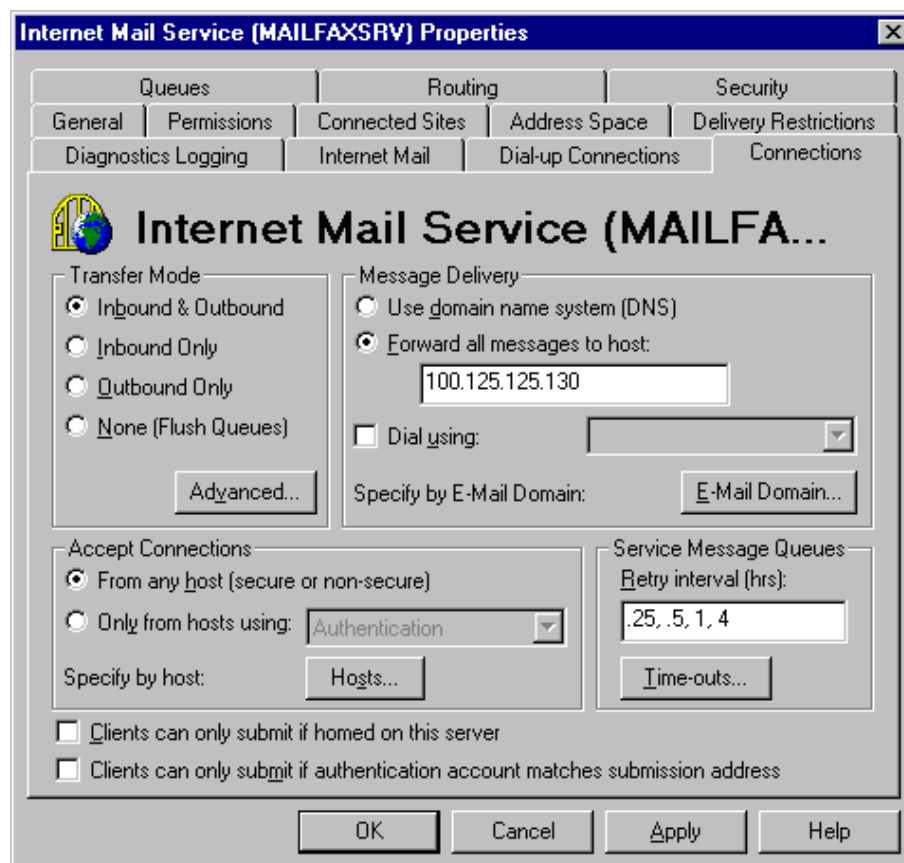
- **Single computer:** Select this option to specify one particular host that will relay email via this server. If you want to look up the IP address of a specific host, click **DNS Lookup**.
- **Group of computers:** Select this option to specify the base IP address for the computers that you want to relay.
- **Domain:** Select this option to include all the computers of a specified domain. This means that the domain controller will openly relay emails via this server. Please note that this option adds processing overhead, and may reduce SMTP service performance because it includes reverse DNS Lookups to verify the domain name of all IP addresses that try to relay.

Step 5: Configure your mail server to relay email via the Gateway server

After you have configured the IIS SMTP service to send and receive email, you must configure your mail server to relay all email to the mail relay server:

If you have Microsoft Exchange Server 4/5/5.5:

1. Start the Microsoft Exchange Administrator and double-click on **Internet Mail Service** to open the properties configuration dialog box.



Screenshot 7 - The Microsoft Internet mail connector

2. Click the **Connections** tab and in the **Message Delivery** area click **Forward all messages to host**. Type the computer name or IP of the machine running GFI MailSecurity.

3. Click **OK** and restart the Microsoft Exchange Server from the services applet.

If you have Microsoft Exchange Server 2000/2003:

You will need to set up an SMTP connection that forwards all email to GFI MailSecurity:

1. Start the Exchange System Manager.
2. Right-click the **Connectors** Node, click **New ► SMTP Connector** and then specify the connector name.
3. Click **Forward all mail through this connector to the following smart host**, type in the IP of the GFI MailSecurity server (the mail relay/Gateway server) and then click **OK**.

NOTE: Always enclose the IP address within square brackets []. For example, [100.130.130.10].

4. Select the SMTP Server that must be associated to this SMTP Connector. Click the **Address Space** tab, and then click **Add**. Click **SMTP** and then click **OK** to accept the changes.
5. Click **OK**. All emails will now be forwarded to the GFI MailSecurity machine.

If you have Lotus Notes:

1. Double-click the **Address Book** in Lotus Notes.
2. Click on Server item to expand its sub-items.
3. Click **Domains** and then click **Add Domains**.
4. In the Basics section, click **Foreign SMTP Domain from the Domain Type field** and in the **Messages Addressed to** area, type "*" in the **Internet Domain** box.
5. Under the **Should be routed to** area, specify the IP of the machine running GFI MailSecurity in the **Internet Host** box.
6. Save the settings and restart the Lotus Notes server.

If you have an SMTP/POP3 mail server:

1. Start the configuration program of your mail server.
2. Search for the option to relay all outbound email via another mail server. This option will be called something like **Forward all messages to host**. Enter the computer name or IP of the machine running GFI MailSecurity.
3. Save the new settings and restart your mail server.

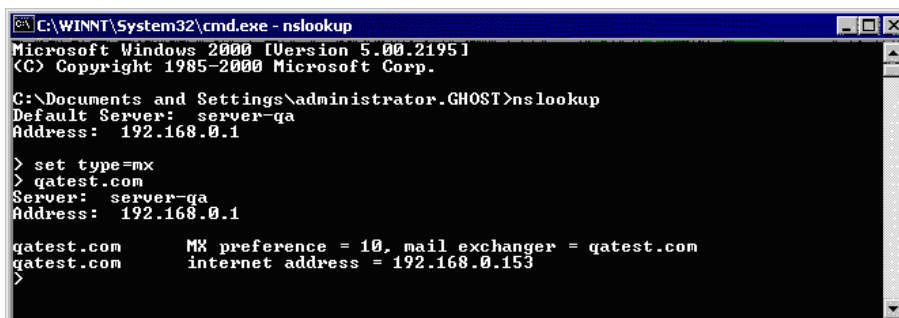
Step 6: The MX record of your domain must point to the mail relay server

NOTE: If your ISP manages the DNS server, ask this provider to update it for you.

Since the new mail relay server must receive all inbound email first, you must update the MX record of your domain to point to the IP of the new mail relay/Gateway server. Otherwise, email will continue to go to your mail server and by-pass GFI MailSecurity.

Verify the MX record of your DNS server as follows:

1. Open the command prompt, type **nslookup** and press Enter.
2. Type **set type=mx** and press Enter.
3. Type your mail domain and press Enter.
4. The MX record should return a single IP that must correspond to the IP of the machine running GFI MailSecurity.



```
C:\WINNT\System32\cmd.exe - nslookup
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\administrator.GHOST>nslookup
Default Server:  server-qa
Address: 192.168.0.1

> set type=mx
> gatest.com
Server:  server-qa
Address: 192.168.0.1

gatest.com      MX preference = 10, mail exchanger = gatest.com
gatest.com      internet address = 192.168.0.153
>
```

Screenshot 8 - Checking the MX record of your domain

Step 7: Test your new mail relay server

Before you proceed to install GFI MailSecurity, verify that your new mail relay server is working correctly.

1. Test the IIS SMTP inbound connection of your mail relay server by sending an email from an external account to an internal user (you can use web-mail, for example MSN Hotmail, if you do not have an external account available). Verify that the email client received the email.
2. Test the IIS SMTP outbound connection of your mail relay server by sending an email to an external account from an email client. Verify that the external user received the email.

NOTE: Instead of using an email client, you can send email manually through Telnet. This will give you more troubleshooting information. For more information, refer to this Microsoft Knowledge Base article:

<http://support.microsoft.com/support/kb/articles/Q153/1/19.asp>

Step 8: Install GFI MailSecurity on the mail relay server

For information on how to install GFI MailSecurity, refer to the 'Installing GFI MailSecurity' section in this chapter.

Preparing to install GFI MailSecurity on your mail server

No additional configuration is required if you are installing GFI MailSecurity directly on your mail server. For information on how to install GFI MailSecurity, refer to the 'Installing GFI MailSecurity' section below.

Installing GFI MailSecurity

Before you install GFI MailSecurity, check the points below:

1. Make sure that you are logged on as Administrator or you are using an account with administrative privileges.

2. Save any pending work and close all open applications on the machine.
3. Check that the machine you are installing GFI MailSecurity on meets the system and hardware requirements specified earlier in this chapter.

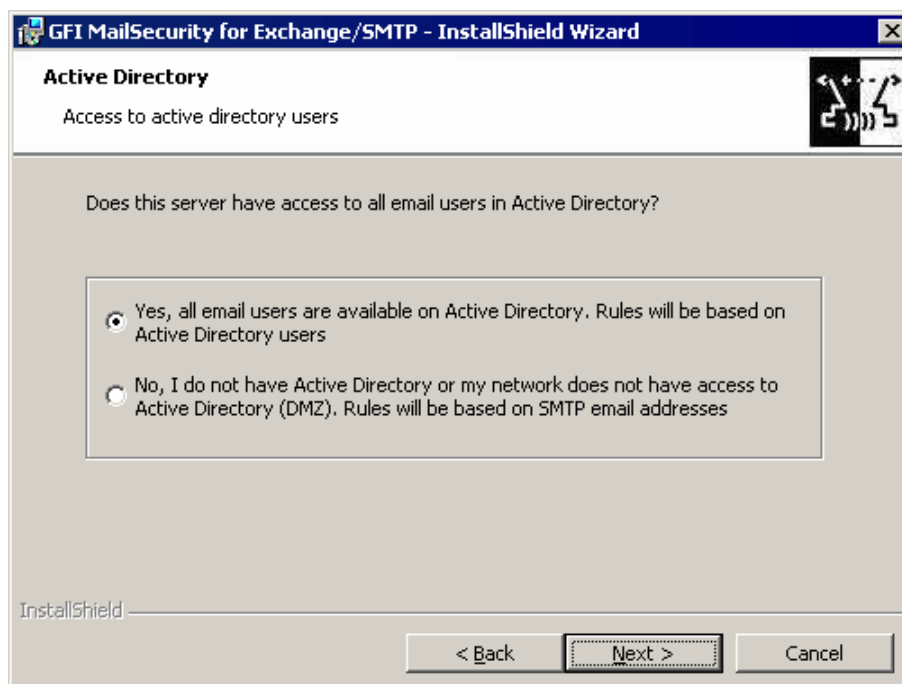
To install GFI MailSecurity follow these steps:

1. Run the GFI MailSecurity setup program by double-clicking on the **MailSecurity10.exe** file. The installation wizard will perform some unpacking operations and then display the **Welcome** page. Click **Next** to continue.
2. Read the license agreement displayed in the **License agreement** page and click **I accept the terms in the license agreement** if you accept the terms of the license agreement. Click **Next** to continue the installation.

NOTE: If upgrading from a previous version than GFI MailSecurity 10 SR8, you will be asked to upgrade to the Firebird database. Selecting import will prompt GFI MailSecurity to automatically launch the quarantine upgrade tool after the installation. If you select not to import the quarantine database, any previous quarantine data will not be used by the upgraded version. For information on the quarantine upgrade tool, refer to the Quarantine Upgrade tool section in this manual.

3. Type the administrator email address in the **Administrator Email** box. If you bought a license for GFI MailSecurity, type it in the **License Key** box. If you do not have a license yet and want to evaluate GFI MailSecurity, leave the default evaluation license key in the **License Key** box. Click **Next** to continue the installation.

NOTE: When you use the evaluation license key, you will be able to use GFI MailSecurity for 10 days. If later you decide to buy GFI MailSecurity, you will not need to install GFI MailSecurity again – entering the purchased license key will be sufficient.

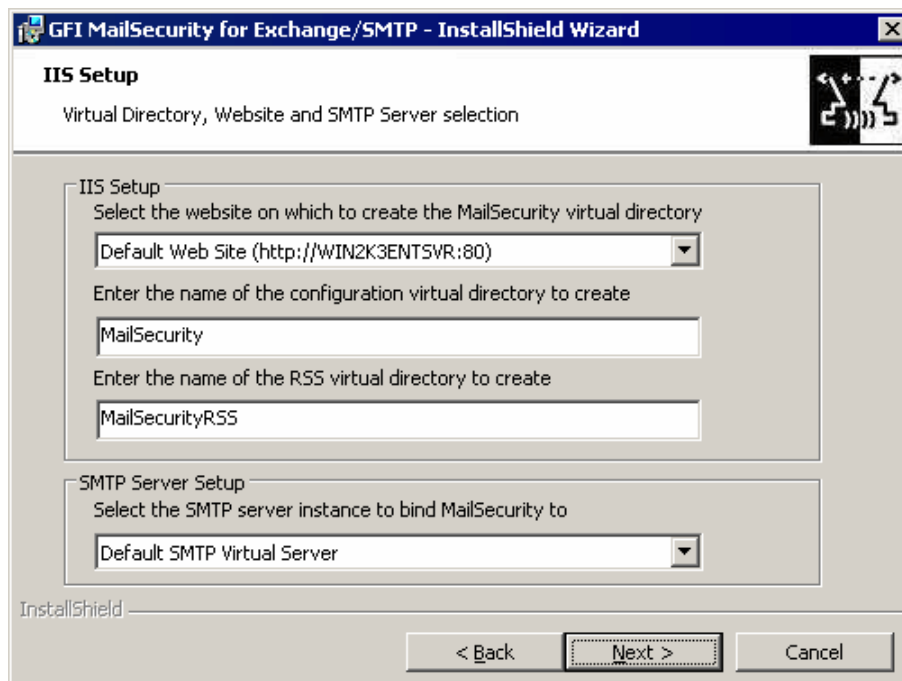


Screenshot 9 - Define if the server has access to all email users in the Active Directory

4. Setup will now ask you to select the mode that GFI MailSecurity will use to retrieve the list of your email users. You must select one of the following options:

- **Yes, all email users are available on Active Directory.** – Select this option to continue installing GFI MailSecurity in **Active Directory mode**. In this mode, GFI MailSecurity creates user-based rules, for example Attachment Checking rules, based on the list of users available in the Active Directory. This means that the machine on which GFI MailSecurity is being installed must be behind your firewall (for example, Mail Server) and must have access to the Active Directory containing all your email users (i.e., the machine on which GFI MailSecurity is being installed must be part of the Active Directory domain).
- **No, I do not have Active Directory or my network does not have access to Active Directory (DMZ).** – Select this option to continue installing GFI MailSecurity in **SMTP mode**. In this mode, GFI MailSecurity will create user-based rules, for example Attachment Checking rules, based on the list of email users/addresses imported from your mail server. You must select this mode if you are installing GFI MailSecurity on a machine that does not have access to the Active Directory containing the complete list of all your email users. This includes machines on a DMZ or machines that are not part of the Active Directory Domain. However, you can still choose this mode to install GFI MailSecurity on machines that do have access to the Active Directory containing all your email users.

Click **Next** to proceed with the installation.



Screenshot 10 - Define your SMTP server and GFI MailSecurity virtual folder details.

5. You now need to select the server where you want to host the GFI MailSecurity configuration pages. On this server, two virtual directories are created to host the configuration pages and the quarantine RSS

feeds. You can specify custom virtual directory names if you want, or else leave the defaults.

NOTE: If you are installing on a Microsoft Exchange Server 2007 machine, the IIS SMTP service is not required, since it has its own built in SMTP server. In such a case, the **SMTP Server Setup** area is not displayed and you can click **Next** to continue and go to step 7 directly.

GFI MailSecurity relies on the IIS SMTP service to send and receive SMTP mail. It binds to your default SMTP virtual server (i.e., the server specified in the MX record of your DNS Server). However, if you have multiple SMTP virtual servers on your domain, you can bind GFI MailSecurity to any available SMTP virtual server. To change the default SMTP connection, select the required server from the list of available SMTP Virtual Servers provided in this dialog box.

NOTE: After installing the product, you can still bind GFI MailSecurity to another SMTP virtual server from the GFI MailSecurity Configuration (**GFI MailSecurity ▶ Settings ▶ Bindings**). For more information, refer to the 'SMTP server bindings' section in the 'General Settings' chapter.

Click **Next** to continue the installation.

6. Setup will now search your network and will import a list of your Local Domains from the IIS SMTP service. GFI MailSecurity determines if an email is inbound or outbound by comparing the domain in a sender's address to the list of local domains. If the address exists in the list, then the email is outbound. Check that all your Local Domains have been included in the list on display. If not, make sure to add any unlisted domain after the installation completes. For more information, refer to the 'Adding local domains' section in the 'General Settings' chapter. Click **Next** to continue.

7. Setup will now ask you to define the folder where you want to install GFI MailSecurity. GFI MailSecurity requires approximately 50 MB of free hard disk space. Additionally, you must also reserve approximately 200 MB for temporary files. Click **Change** to specify a new installation path or click **Next** to install in the default location and proceed with the installation.

NOTE: If you are installing GFI MailSecurity on a x64 machine, it will be installed under the c:\program files (x86)\ folder.

8. The installation wizard has now collected all the required installation settings and is ready to install GFI MailSecurity. If you want to make changes to these settings, click **Back**. Otherwise, click **Install** to start the installation process.

9. During the installation, you are prompted that the setup needs to restart the SMTP services. Click **Yes** to restart these services and finalize the installation.

NOTE: If you are installing on a Microsoft Exchange Server 2007 machine, you will not be prompted to restart the SMTP service.

10. When the installation completes, click **Finish** to close the installation wizard.

NOTE 1: If you are installing on a Microsoft Exchange Server 2007 machine, the installation will launch the GFI MailSecurity Post-

Installation Wizard. Refer to the following section for information on how to use this wizard.

NOTE 2: If you are upgrading from a previous version (version 9 onwards) of GFI MailSecurity, you might be prompted to upgrade your quarantine database to a new Firebird database format. For more information, refer to the Quarantine Upgrade tool section in this manual.

GFI MailSecurity Post-Installation Wizard

NOTE: This section applies only when installing GFI MailSecurity on a Microsoft Exchange Server 2007 machine.

IMPORTANT: You need to complete this wizard for GFI MailSecurity to work with Microsoft Exchange Server 2007.

The GFI MailSecurity installation wizard launches the GFI MailSecurity Post-Installation Wizard when you click **Finish**. The GFI MailSecurity Post-Installation Wizard registers GFI MailSecurity with the local installation of Microsoft Exchange Server 2007 so that it can process and scan the emails passing through the server.

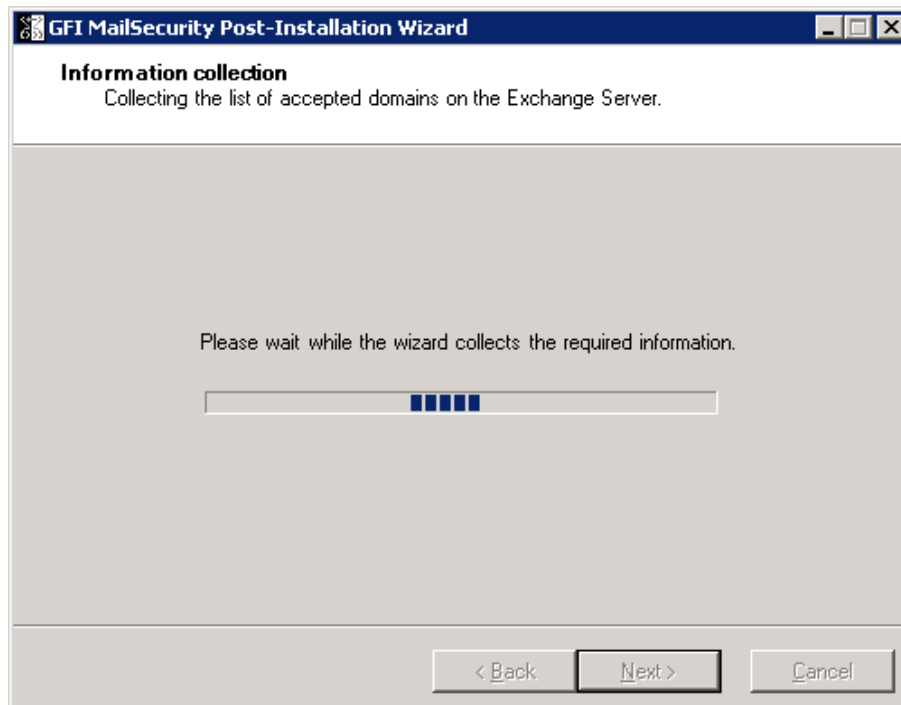
To complete the GFI MailSecurity Post-Installation Wizard, follow these steps:

1. Click **Next** in the welcome page.



Screenshot 11 - GFI MailSecurity Post-Installation Wizard welcome page

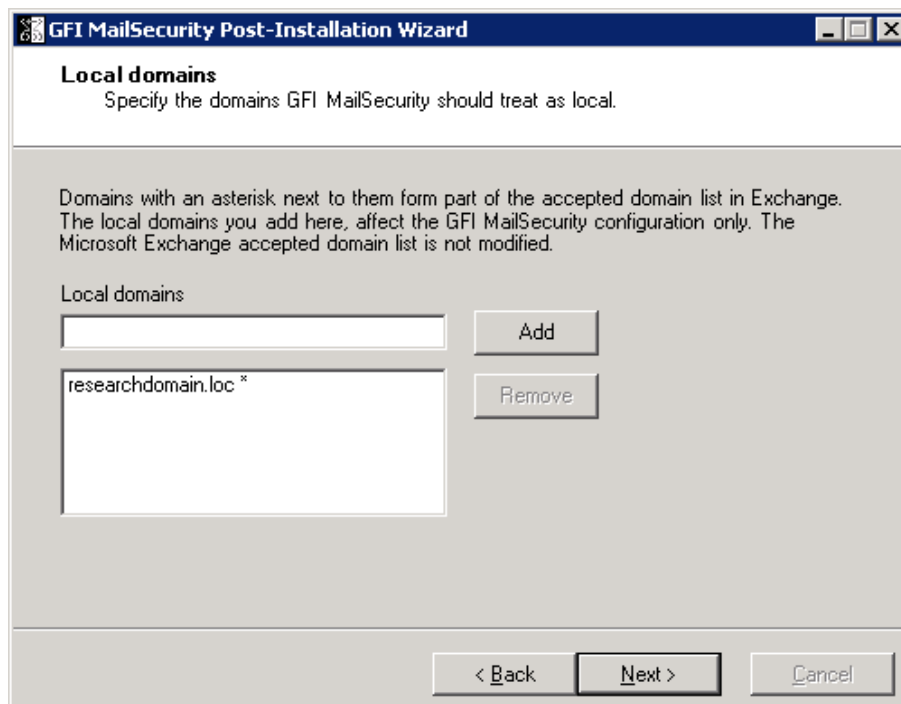
2. The wizard will collect information from the Microsoft Exchange Server 2007 installation, such as the list of local domains and the server roles installed, for example Hub Transport Server Role.



Screenshot 12 – Collecting information from Microsoft Exchange Server 2007

3. The wizard will display the accepted domain list collected from Microsoft Exchange Server 2007. If you need to specify another local domain, type it in the **Local domains** box and click **Add**. If you want to remove a domain that you added from this page, click on it from the list, and then click **Remove**.

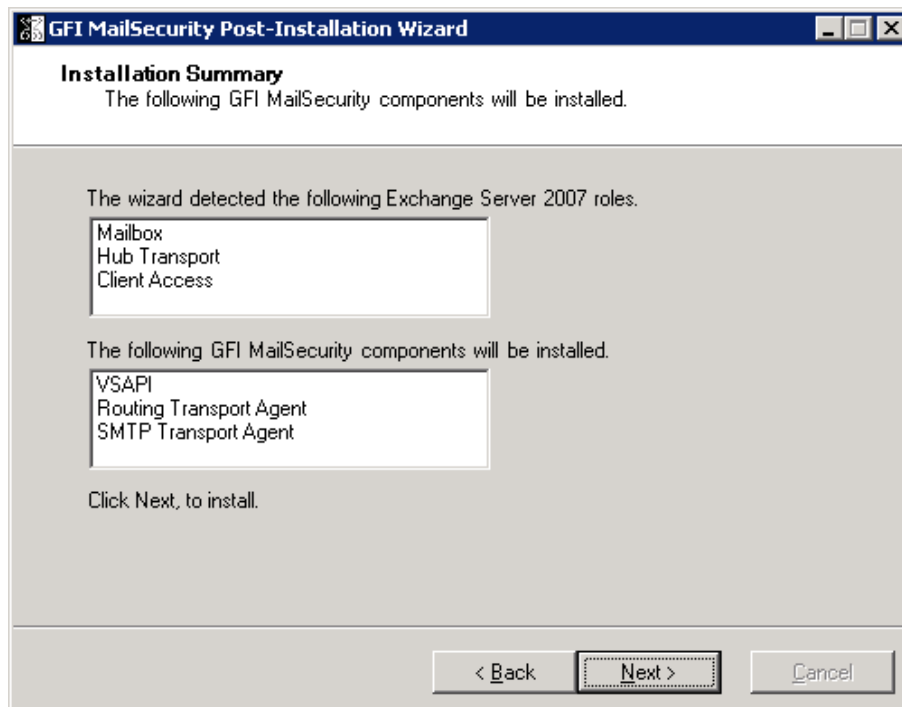
NOTE: The local domains you add from this page affect the GFI MailSecurity installation only. The Microsoft Exchange Server 2007 accepted domains list is not modified.



Screenshot 13 - Local domains list

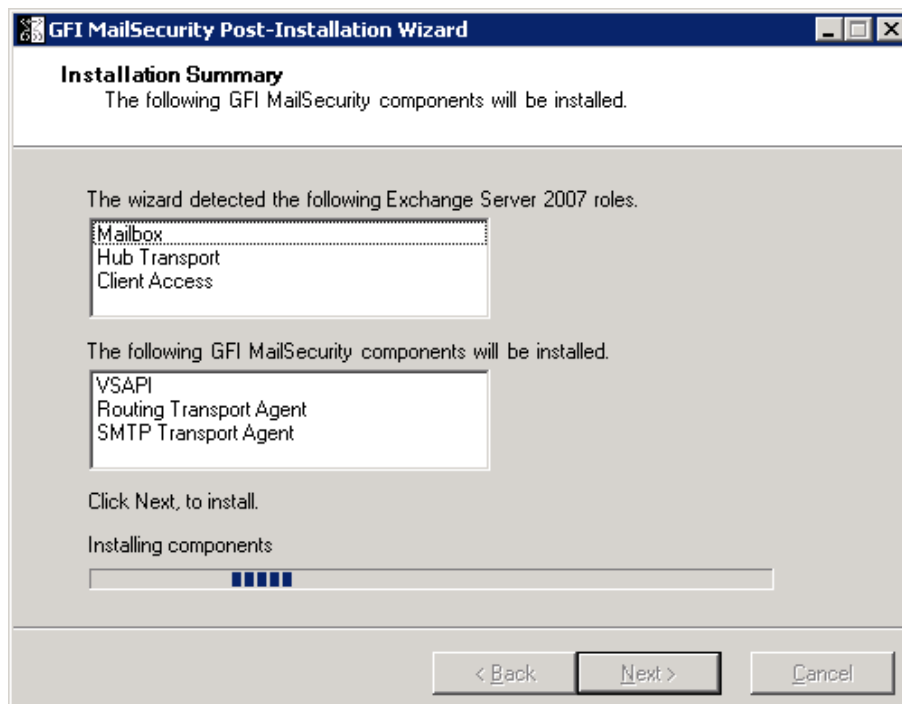
4. Click **Next** to continue.

5. The wizard displays a list of the Microsoft Exchange Server 2007 server roles detected on this machine, and a list of the GFI MailSecurity components it needs to register for it to be able to process and scan emails passing through the server.



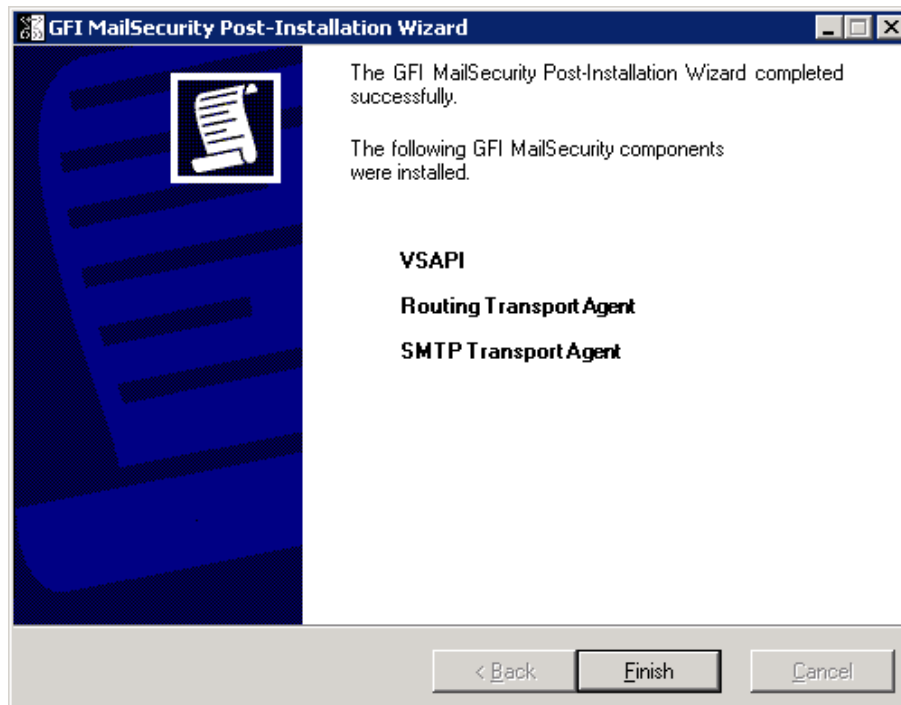
Screenshot 14 - Server roles detected and list of components to install.

6. Click **Next** to install the required GFI MailSecurity components.



Screenshot 15 - Installing the required GFI MailSecurity components

7. In the finish page, the GFI MailSecurity Post-Installation wizard will list the GFI MailSecurity components that it successfully installed. Click **Finish** to close the wizard and complete the installation of GFI MailSecurity on a Microsoft Exchange Server 2007 machine.



Screenshot 16 - GFI MailSecurity Post-Installation Wizard finish page

Adding GFI MailSecurity to the Windows DEP Exception List

Data Execution Prevention (DEP) is a set of hardware and software technologies that perform memory checks to help prevent malicious code from running on a system.

The DEP technology is available only on Microsoft Windows XP with Service Pack 2, Microsoft Windows Server 2003 (x32 Edition) with Service Pack 1 and Microsoft Windows Server 2003 (x64 Edition). On Microsoft Windows Server 2003 (x32 Edition) with Service Pack 1 and Microsoft Windows Server 2003 (x64 Edition), DEP is by default turned on for all programs and services except those that the administrator selects.

If you installed GFI MailSecurity on Microsoft Windows Server 2003 (x32 Edition) with Service Pack 1 or Microsoft Windows Server 2003 (x64 Edition), you will need to add the GFI MailSecurity scanning engine executable (**GFiScanM.exe**) and the Kaspersky Virus Scanning Engine executable (**kavss.exe**) to the Windows Data Execution Prevention (DEP) exception list.

To add the GFI executables in the DEP exception list follow these steps:

1. From the **Start** menu load the **Control Panel** and choose the **System** applet.
2. From the **Advanced** tab, click **Settings** under the **Performance** area.
3. Click the **Data Execution Prevention** tab.
4. Click **Turn on DEP for all programs and services except those I select**.

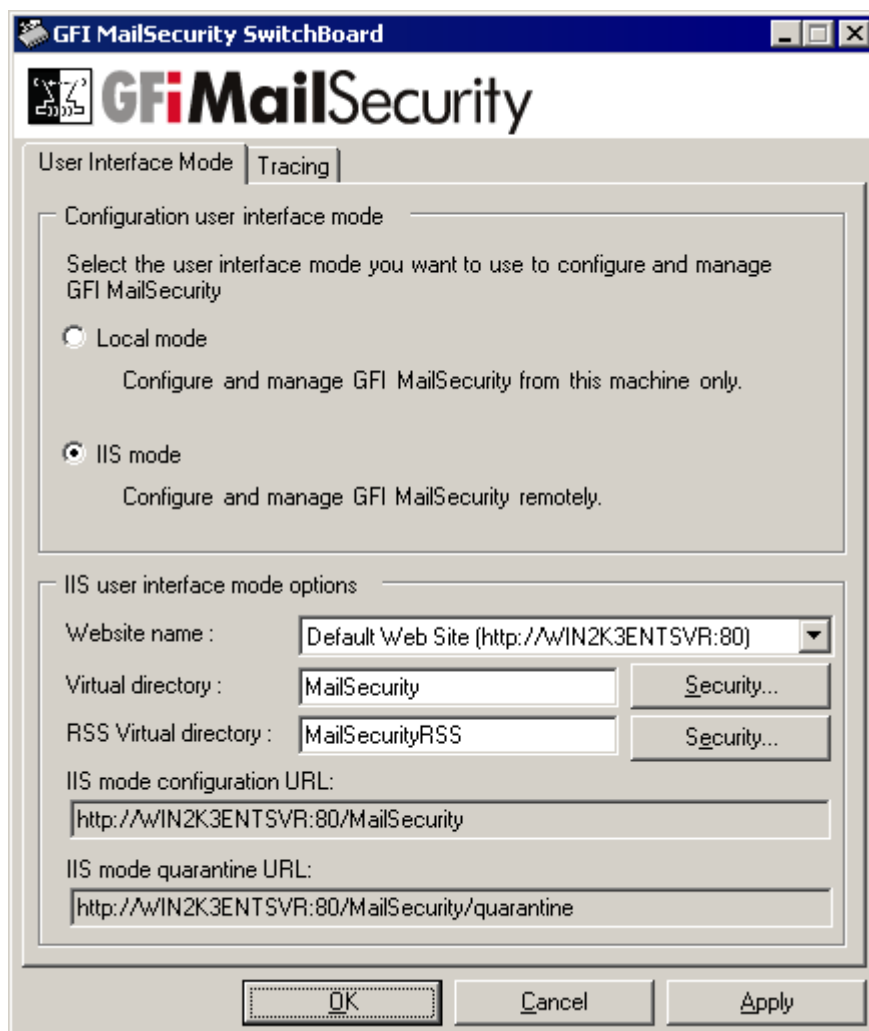
5. Click **Add** and from the dialog box browse to the GFI MailSecurity installation folder, <GFI\ContentSecurity\MailSecurity>, and choose **GFIScanM.exe**.
6. Click **Add** and from the dialog box browse to the GFI MailSecurity installation folder, <GFI\ContentSecurity\AntiVirus\Kaspersky\>, and choose **kavss.exe**.
7. Click **Apply** and **OK** to apply the changes.
8. Restart the "GFI Content Security Auto-Updater Service" and the "GFI MailSecurity Scan Engine" services.

Securing access to the GFI MailSecurity configuration/quarantine

The GFI MailSecurity configuration and quarantine store can be accessed through a web browser and thus it is imperative that you configure proper access security so that only authorized users can set-up rules and manage the quarantine store.

You can configure access security to the GFI MailSecurity configuration pages and quarantine store via the GFI MailSecurity SwitchBoard application. To configure access security, follow these steps:

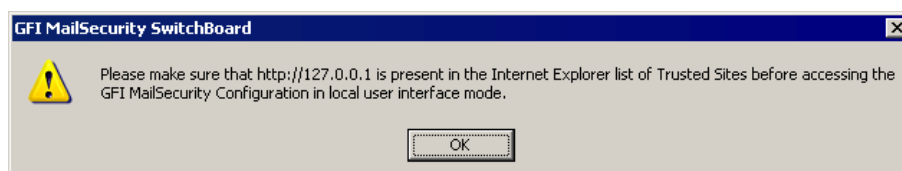
1. Click the **GFI MailSecurity SwitchBoard** shortcut found under **Start ► Programs ► GFI MailSecurity**.
2. The **GFI MailSecurity SwitchBoard** application is loaded. You now need to select whether you want to allow only local access to the Configuration and Quarantine Store or else both local and remote. To allow only local access, click **Local mode**, so that the Configuration and Quarantine Store can only be accessed when working directly on the server machine where GFI MailSecurity is installed. On the other hand, to allow both local and remote access, click **IIS mode**, so that authorized users, both from the local machine and other remote machines, can access the GFI MailSecurity Configuration and Quarantine Store.



Screenshot 17 - GFI MailSecurity SwitchBoard

3. If you selected **Local mode**, you do not need to configure anything else. If you selected **IIS mode** you now need to configure the Active Directory accounts or groups that have access to the Configuration and Quarantine Store, and you can change the virtual directory name where the GFI MailSecurity pages are stored.

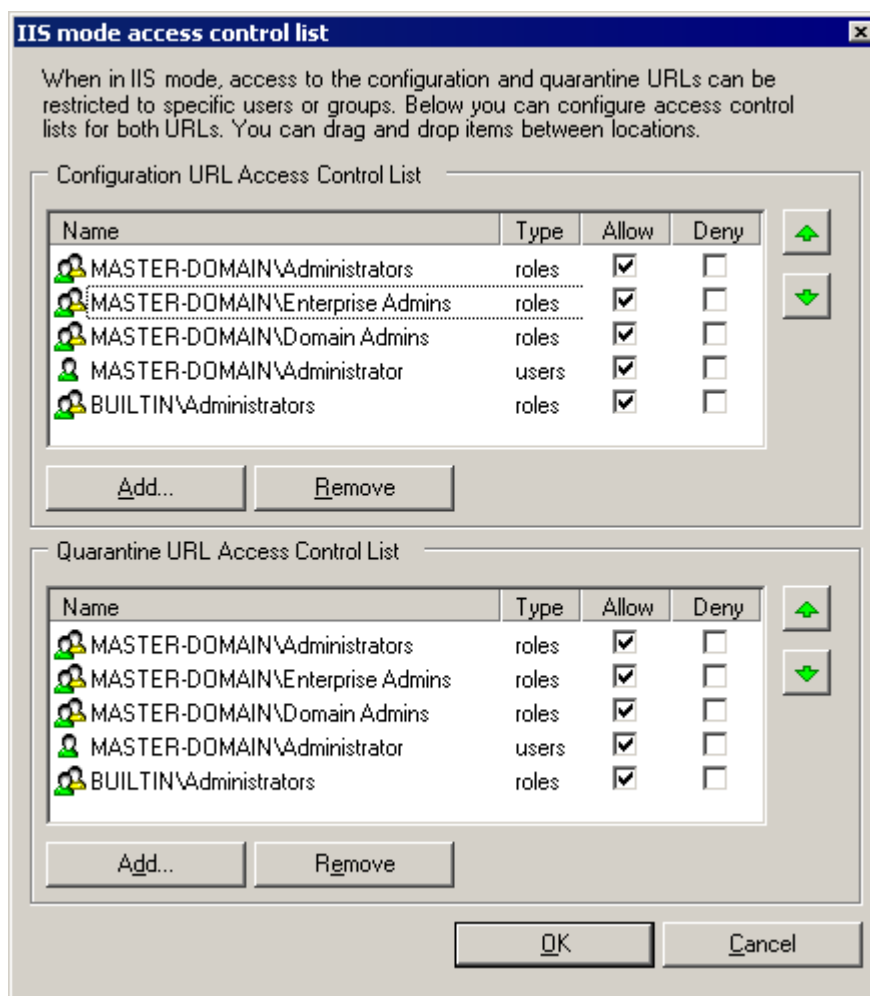
NOTE: If you select **Local mode** you need to add 'http://127.0.0.1' to the list of trusted sites in Internet Explorer. For further information, refer to the 'Adding local host to the trusted sites list' section below.



Screenshot 18 - Local host address must be added to trusted sites list

4. To configure access security, click **Security...** next to the **Virtual Directory** box.

5. In the **IIS mode access control list** dialog box you can configure who gets access to the configuration pages and the quarantine store in separate access control lists.



Screenshot 19 - Configuration / Quarantine store Access Control Lists

6. To configure the accounts that get access to the configuration pages, use the **Add** and **Remove** buttons underneath the **Configuration URL Access Control List**. If you want to deny access to a listed account without removing it from the list, select the check box under the **Deny** column.

7. To configure the accounts that get access to the quarantine store, use the **Add** and **Remove** buttons underneath the **Quarantine URL Access Control List**. If you want to deny access to a listed account without removing it from the list, select the check box under the **Deny** column.

NOTE: To avoid reselecting the same accounts twice, once for each list, you can easily drag and drop accounts and groups between the two lists.

8. When ready click **OK**.

9. If you want to specify a different virtual directory name, you can do so by editing the entry in the **Virtual directory** box.

10. Click **OK** to save your changes. A progress bar shows you the progress while applying the new settings.



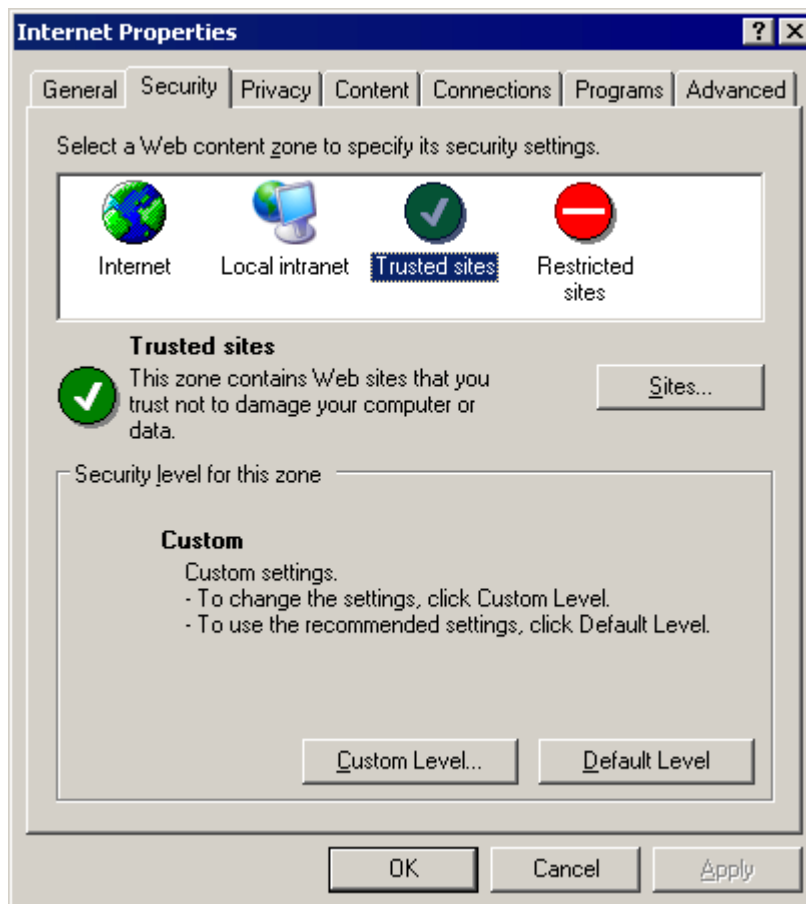
Screenshot 20 - New SwitchBoard settings successfully applied

11. When the process completes, click **OK**.

Adding local host to the trusted sites list

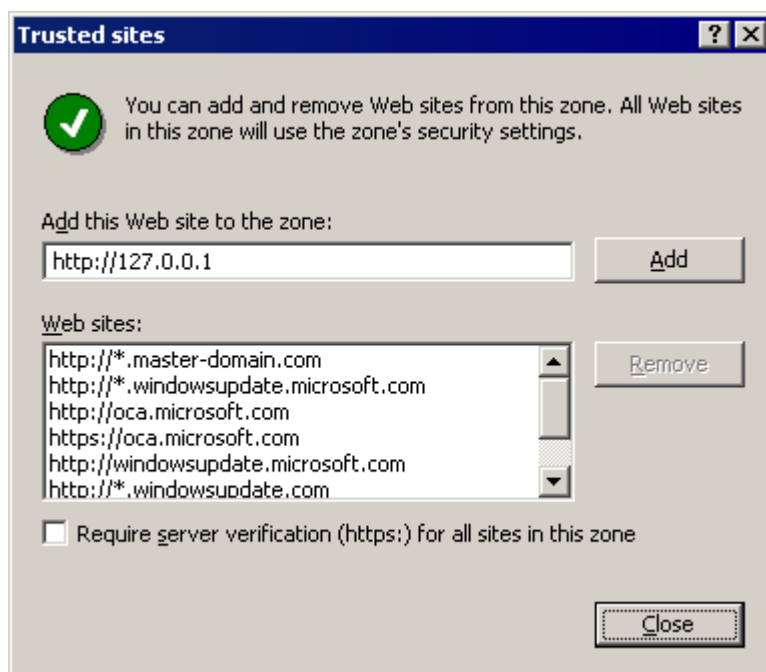
When you configure GFI MailSecurity to be accessible only locally, you need to add the local host address, 'http://127.0.0.1', to the list of trusted sites in Internet Explorer. To do this, follow these steps:

1. Click the **Control Panel** shortcut under the **Start** menu.
2. From the **Control Panel** open the **Internet Options** applet.
3. In the **Internet Properties** dialog box click the **Security** tab and then click the **Trusted sites** icon from the **Web content zone** list.



Screenshot 21 - Internet properties dialog

4. Click **Sites**.
5. In the **Trusted sites** dialog box specify 'http://127.0.0.1' in the **Add this Web site to the zone** box.
6. Click **Add**. The local host address is added to the **Web sites** list.



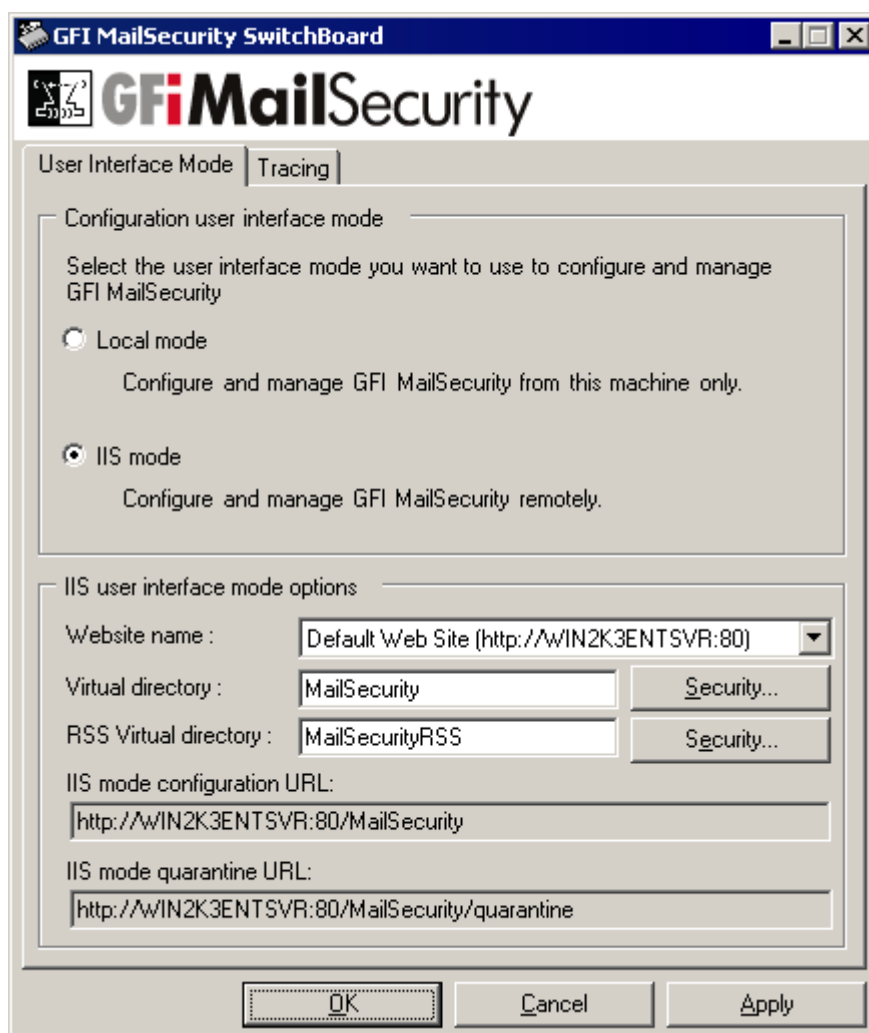
Screenshot 22 - Trusted sites dialog

7. Click **Close**.
8. Click **OK** in the **Internet Properties** dialog box to close it and save the new settings.

Securing access to the GFI MailSecurity Quarantine RSS feeds

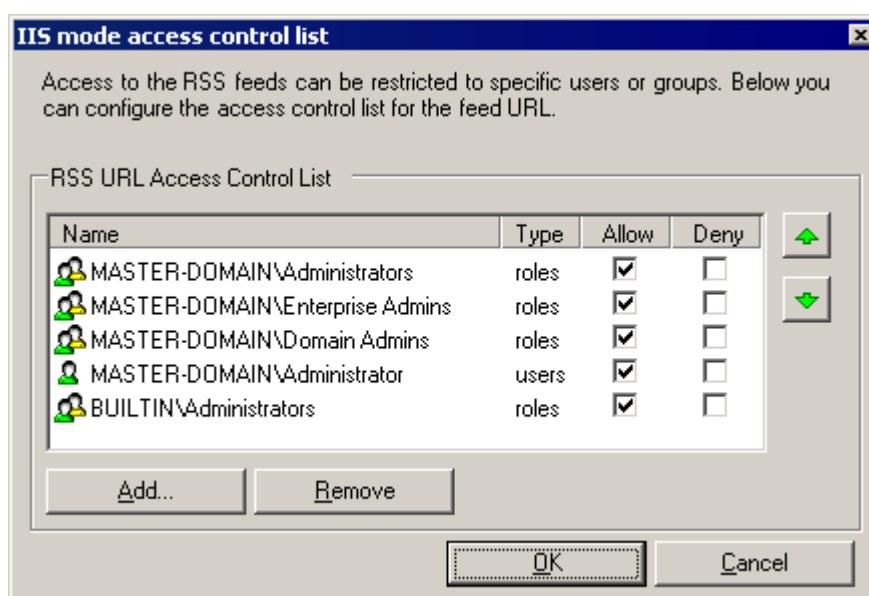
You can configure GFI MailSecurity to create quarantine RSS feeds on specific quarantine folders. To configure who can subscribe to the quarantine RSS feeds, follow these steps:

1. Click the **GFI MailSecurity SwitchBoard** shortcut found under **Start ► Programs ► GFI MailSecurity**.
2. In the **GFI MailSecurity SwitchBoard** dialog box, click **Security** next to the **RSS Virtual Directory** box.



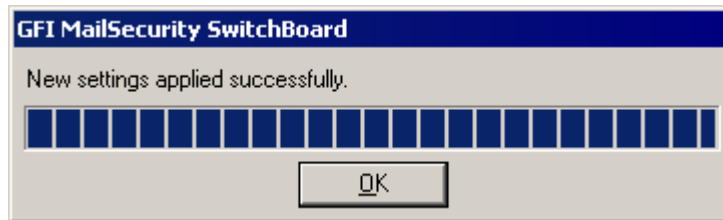
Screenshot 23 - GFI MailSecurity SwitchBoard

3. In the **IIS mode access control list** dialog box you can configure who can subscribe to the quarantine RSS feeds.



Screenshot 24 – Quarantine RSS feeds Access Control Lists

4. Use the **Add** and **Remove** buttons underneath the **RSS URL Access Control List**. If you want to deny access to a listed account without removing it from the list, select the check box under the **Deny** column.
6. When ready click **OK**.
7. If you want to specify a different virtual directory name, you can do so by editing the entry in the **RSS Virtual directory** box.
8. Click **OK** to save your changes. A progress bar shows you the progress while applying the new settings.



Screenshot 25 - New SwitchBoard settings successfully applied

9. When the process completes, click **OK**.

Accessing the GFI MailSecurity Configuration and Quarantine Store

This section will show you how to access the GFI MailSecurity Configuration and Quarantine Store from the local machine or a remote machine.

Accessing the configuration from the GFI MailSecurity machine

To access the GFI MailSecurity configuration or quarantine store from the same machine where GFI MailSecurity is installed, i.e. locally, follow these steps:

1. Click the **GFI MailSecurity** shortcut found under **Start ► Programs ► GFI MailSecurity**.
2. If you have configured GFI MailSecurity to be accessible only locally, via the GFI MailSecurity SwitchBoard application, a viewer application will automatically load up displaying the GFI MailSecurity configuration and quarantine store.



Screenshot 26 - GFI MailSecurity accessed under local mode only

Accessing the configuration from a remote machine

To access the GFI MailSecurity configuration or quarantine store from a remote machine, follow these steps:

1. Start Microsoft Internet Explorer.
2. In the address bar, specify the following address:

'http://<machine name>/<virtual directory name>' to access the configuration or 'http://<machine name>/<virtual directory name>/quarantine' to access the quarantine store directly.

For example:

'http://win2k3entsvr.master-domain.com/mailsecurity' for the configuration or 'http://win2k3entsvr.master-domain.com/mailsecurity/quarantine' for the quarantine store.

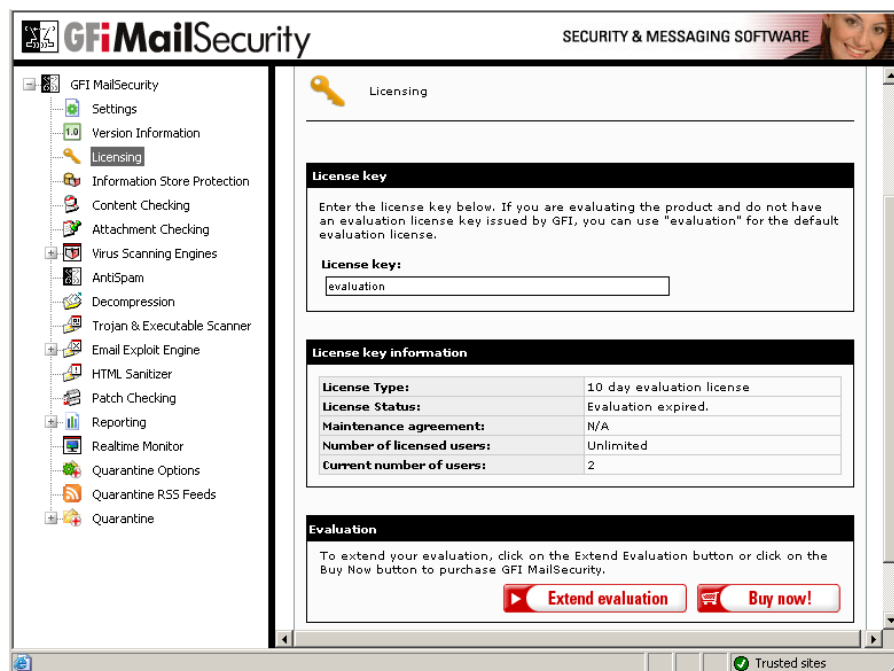
3. You will be prompted to specify a user name and password to authenticate and determine whether you have access to the page requested. If the account specified has access, the GFI MailSecurity configuration or quarantine store is displayed.



Screenshot 27 - GFI MailSecurity accessed under IIS mode

Entering your license key after installation

The unregistered, evaluation version of GFI MailEssentials expires after 10 days.



Screenshot 28 - License key information

When you obtain the 30-day evaluation key or the purchased licensed key, you can enter your license key in the **GFI MailSecurity ▶ Licensing** node, without having to re-install the product.

Entering the license key should not be confused with the process of registering your company details on our website. This is important, since it allows us to give you support, and notify you of important product news. Register at <http://www.gfi.com/pages/regfrm.htm>.

Upgrading from GFI MailSecurity 8 to GFI MailSecurity 10

Due to fundamental architectural changes between GFI MailSecurity 10 and GFI MailSecurity 8, it is not possible to install GFI MailSecurity 10 on top of an existing installation of GFI MailSecurity 8.

This section therefore shows you how to:

- Replace your current GFI MailSecurity 8 installation with GFI MailSecurity 10.
- Convert and import the GFI MailSecurity 8 configuration settings to GFI MailSecurity 10's new configuration database format.

NOTE: If GFI MailSecurity 8 was installed in SMTP mode and GFI MailSecurity 10 is installed in Active Directory mode, you will not be able to convert and import the settings due to user-based rules. This also applies if GFI MailSecurity 8 was installed in Active Directory mode and GFI MailSecurity 10 is installed in SMTP mode.

To upgrade from GFI MailSecurity 8 to GFI MailSecurity 10, follow these steps:

1. Uninstall GFI MailSecurity 8.
2. When the GFI MailSecurity 8 uninstallation completes, certain files are left behind under the root folder where GFI MailSecurity 8 was installed. One of these files is the `avapicfg.rdb` file located in the Data sub-folder.

NOTE: Do not delete this file since it contains the GFI MailSecurity 8 configuration settings. You will need this file to migrate the settings from GFI MailSecurity 8 to GFI MailSecurity 10.

3. Install GFI MailSecurity 10 as shown in the 'Install GFI MailSecurity' section of this chapter.

NOTE: To install GFI MailSecurity 10, you need to have the following installed on the machine:

- Microsoft .Net framework 1.1 / 2.0
- MSMQ – Microsoft Messaging Queuing Service.
- Internet Information Services (IIS) – SMTP service and World Wide Web service.

NOTE: Do not install GFI MailSecurity 10 to the same path where GFI MailSecurity 8 was installed, to prevent files such as `avapicfg.rdb` from being overwritten.

4. After the installation of GFI MailSecurity 10 is complete, you need to stop all GFI-related services along with the IIS Admin service, from the Services control applet. Then you can run the GFI MailSecurity 8 settings migration tool.

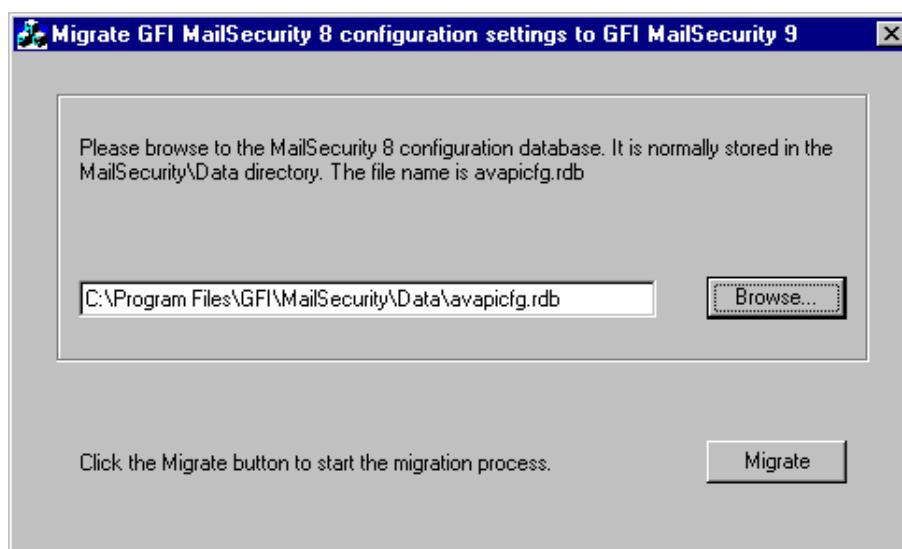
NOTE: You must stop the following services before going on to the next step:

- GFI Content Security Attendant Service

- GFI Content Security Auto-Updater Service
- GFI MailSecurity Attendant Service
- GFI MailSecurity Scan Engine
- IIS Admin
- Simple Mail Transfer Protocol (SMTP).

5. To convert and import the GFI MailSecurity 8 settings to the GFI MailSecurity 10 configuration database, you need to run the msec8upg.exe tool found in the GFI MailSecurity 10 folder, for example:

c:\program files\GFI\ContentSecurity\MailSecurity.



Screenshot 29 - GFI MailSecurity 8 configuration settings migration tool

6. Double-click the msec8upg.exe file.


7. When the tool loads, click **Browse**. Select the avapicfg.rdb file from the data sub-folder under the GFI MailSecurity 8 root folder.

8. Click **Migrate**.

NOTE: If you click **Migrate** and the user lookup mode of GFI MailSecurity 8 and GFI MailSecurity 10 do not match (for example GFI MailSecurity 8 was installed in SMTP mode and GFI MailSecurity 10 is installed in Active Directory mode or vice versa), an error like the one shown below will be displayed. In such a case, you will not be able to convert and import the settings due to user-based rules.



Screenshot 30 - User lookup mode mismatch.

9. When the migration process completes, a **Configuration was successfully converted** information dialog box will be displayed. Click **OK** to close the information dialog box and click the close button  to close the migration tool.

10. You now need to start all the services that you stopped in step 4 above, from the Services control applet.
11. Use the GFI MailSecurity 10 configuration to check that the GFI MailSecurity 8 settings were migrated correctly.

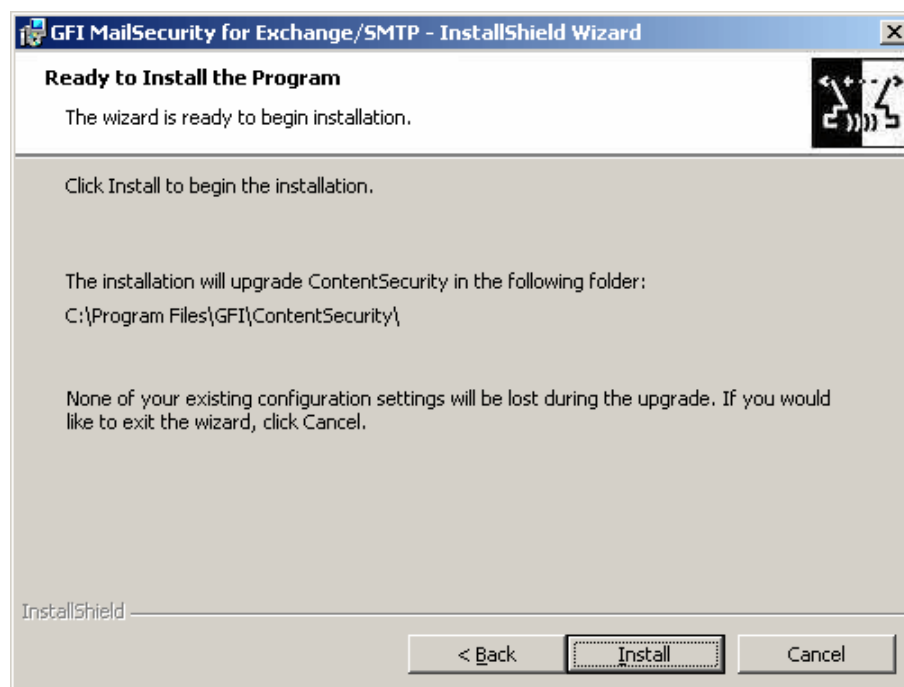
Upgrading from GFI MailSecurity 9 to GFI MailSecurity 10

NOTE: The upgrade process cannot be reverted. If you upgrade GFI MailSecurity to version 10, you cannot go back to version 9 of the product.

If you are currently using GFI MailSecurity 9, you can upgrade your current installation. The GFI MailSecurity 9 configuration settings are kept. You need to enter the fully purchased license key after the upgrade completes. For information on how to obtain the new license key, visit <http://customers.gfi.com>.

To upgrade:

1. Launch the GFI MailSecurity 10 setup file on the machine on which you have installed GFI MailSecurity 9.
2. Setup will now proceed to install GFI MailSecurity 10 in exactly the same manner as a new installation. However, it will not let you change the destination folder.



Screenshot 31 - Upgrading from GFI MailSecurity 9 to GFI MailSecurity 10

3. To continue the installation, click **Install**. For a detailed description, of the installation procedure, refer to the 'Installing GFI MailSecurity' section earlier in this chapter.

NOTE: During an upgrade you are also asked to upgrade your quarantine database to the new Firebird database format. For more information, refer to the Quarantine Upgrade tool section in this manual.

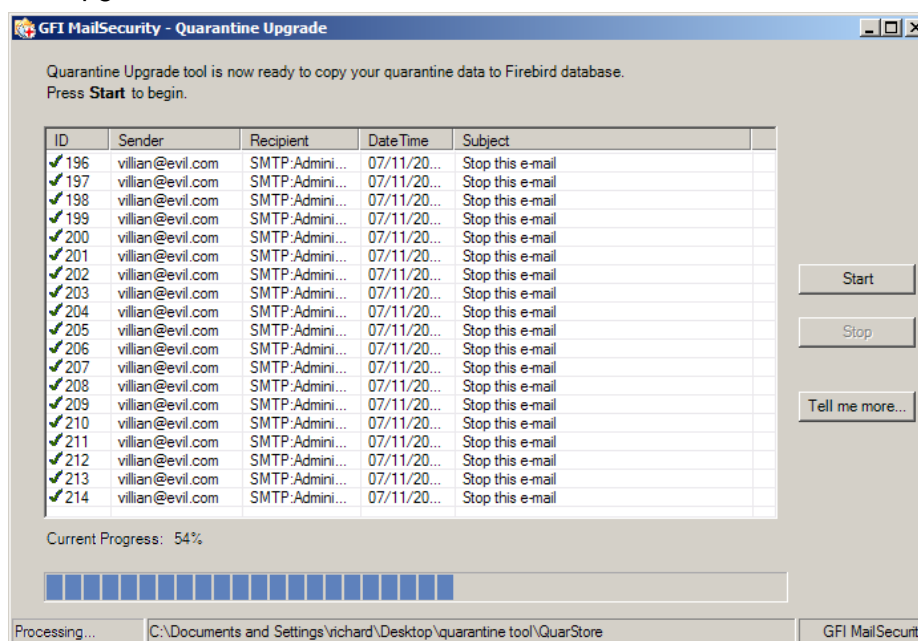
Quarantine Upgrade tool

Starting from GFI MailSecurity 10 SR8, Quarantine information is stored in a Firebird database format instead of Microsoft Access database. For upgrades between version 9 and 10 and between previous builds of version 10 to GFI MailSecurity 10 SR8, the Quarantine upgrade tool automates to the migration of pre-existing quarantine data to the new Firebird database format.

NOTE: The old quarantine data will not be available until imported.

Using the quarantine upgrade tool

The Quarantine upgrade tool is automatically launched after installing the upgrade to GFI MailSecurity SR8. In case you need to launch it manually, navigate to the GFI MailSecurity installation folder (typically Program Files\GFI\ContentSecurity\MailSecurity\) and run QssUpgrade.exe



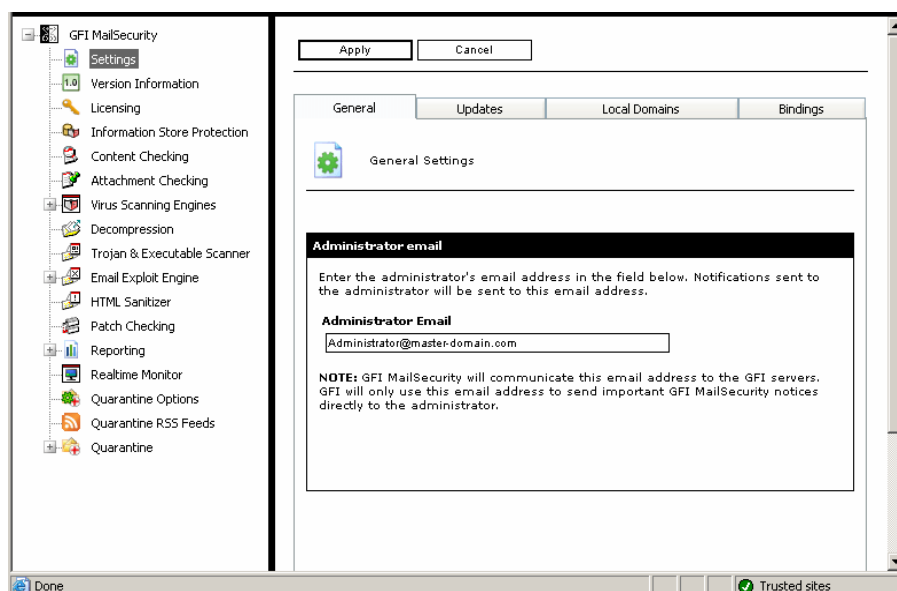
Screenshot 32 - Quarantine upgrade tool

1. Press **Start** button to start data migration.
2. Press **Pause/Continue** button to pause or continue data processing.
3. Press **Stop** button to cancel your data migration and restart at a later stage by pressing Start again.

NOTE: Upgrading your quarantine to the firebird database format might take long depending on the volume of your quarantine data.

General settings

Introduction to settings



Screenshot 33 - GFI MailSecurity general settings page

The **Settings** node allows you to configure a number of general options, including the administrator's email address, the Update URLs, the list of Local Domains, the SMTP server bindings and the management of the user list when GFI MailSecurity is installed in SMTP mode only. To configure the general settings, click the **GFI MailSecurity ► Settings** node.

Define the administrator's email address

GFI MailSecurity can be configured to send email notifications to the administrator whenever a security threat is found in an email. To set up the administrator's notification address:

1. Click the **Settings** node to open the **General Settings** page in the right window.
2. In the **General** tab, specify the email address where you wish to send email notifications addressed to the administrator in the **Administrator Email** box.
3. Click **Apply**.

Configuring proxy server settings for automatic updates

GFI MailSecurity will automatically search and download updates (for example, virus definitions updates and Trojan & Executable Scanner definitions updates) from the GFI update servers.

If the server on which GFI MailSecurity is installed, connects to the internet through a proxy server, you need to configure the proxy server settings as follows:

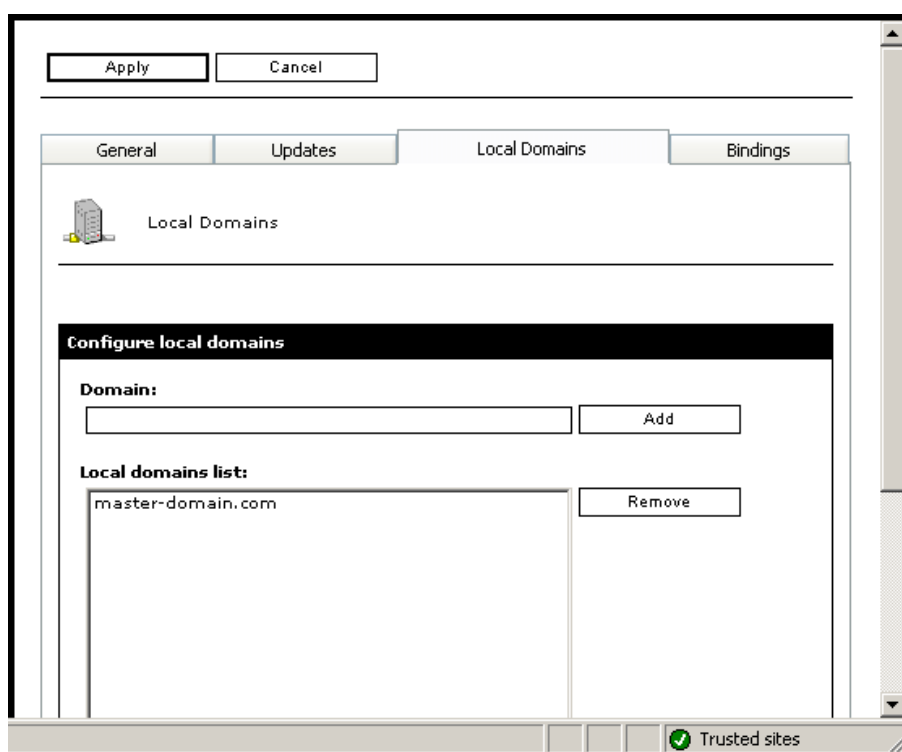
1. Click the **Settings** node to open the general settings page.
2. Click the **Updates** tab.
3. Select the **Enable proxy server** check box. In the **Proxy server** and **Port** boxes specify the Machine Name / IP of the proxy server and the port to connect on respectively. If the proxy server requires authentication, select the **Enable proxy authentication** check box and specify the user name and password in the **Username** and **Password** boxes respectively.

The screenshot displays two configuration panels. The top panel, titled "Proxy server settings", contains the instruction "Configure proxy settings" and an unchecked checkbox labeled "Enable proxy server". Below this are input fields for "Proxy server:" and "Port:", with the value "8080" entered in the port field. The bottom panel, titled "Proxy authentication settings", contains the instruction "Configure proxy authentication settings" and a checked checkbox labeled "Enable proxy authentication". Below this are input fields for "Username:" and "Password:", with the password field masked with asterisks. A note at the bottom of the second panel states: "* For security reasons, the length in the password box above does not necessarily reflect the true password length".

Screenshot 34 - Updates server proxy settings

4. Click **Apply**.

Adding Local Domains



Screenshot 35 - Local Domains list

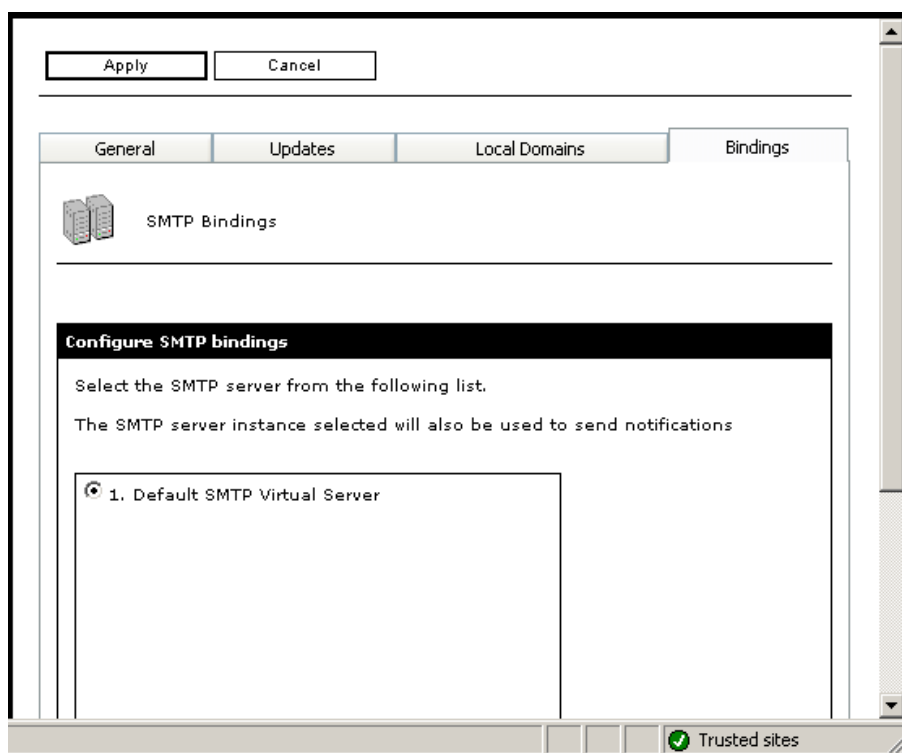
GFI MailSecurity needs to know what your local domains are to be able to classify an email as inbound or outbound. During installation, GFI MailSecurity will import local domains from the IIS SMTP service. If, however, you wish to add or remove local domains afterwards, you must follow these steps:

1. Click the **Settings** node to open the general settings page.
2. Click the **Local Domains** tab and specify the name of the domain in the **Domain** box.
3. Click **Add** to include the stated domain in the **Local domains list**. If you want to remove a listed domain, select it from the list and click **Remove**.
4. Click **Apply**.

NOTE: You can use the local domains option if you want to configure local mail routing in IIS differently, for example, to add domains that are local for mail routing purposes but which are not local for your mail server.

SMTP server bindings

NOTE: The SMTP Server bindings tab is not visible when GFI MailSecurity is installed on a Microsoft Exchange Server 2007 machine.



Screenshot 36 - Binding GFI MailSecurity to a different SMTP Server

GFI MailSecurity relies on the IIS SMTP service to send and receive SMTP mail. By default, it binds to your default SMTP virtual server. However, if you have multiple SMTP virtual servers installed on your machine, you can select to which one you want to bind GFI MailSecurity. You can select your virtual SMTP server both during the installation stage as well as from the **Bindings** tab after the installation. To change the current SMTP Virtual Server:

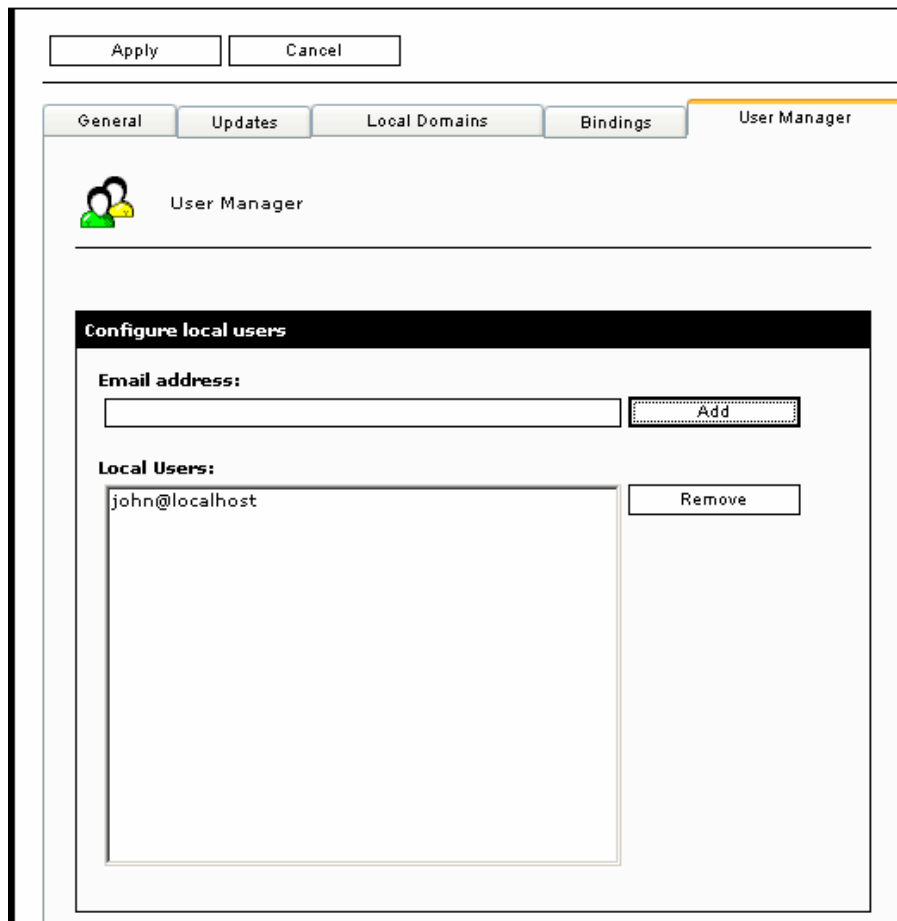
1. Click the **Settings** node to open the general settings page in the right window.
2. Click the **Bindings** tab and select the required SMTP Virtual Server from the available list of servers present in your domain.
3. Click **Apply**.

For more information on how to configure your SMTP service, refer to the 'Installing and configuring IIS SMTP & World Wide Web services' section earlier in the manual.

Managing local users in SMTP mode

When you install GFI MailSecurity in Active Directory mode, the list of local users is stored in the Active Directory store. When you choose to install GFI MailSecurity in SMTP mode, the list of local users is stored in a database managed by GFI MailSecurity.

To populate and manage the user list when GFI MailSecurity is installed in SMTP mode, a **User Manager** is available under the **Settings** node.



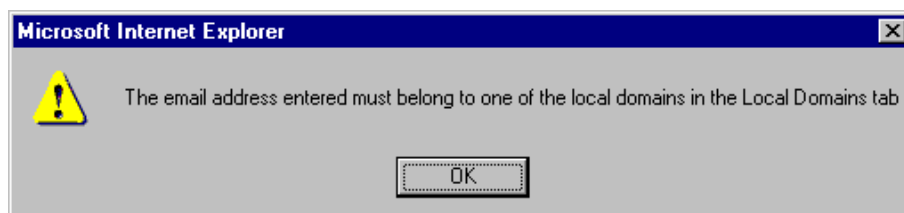
Screenshot 37 - User Manager

The **User Manager** tab displays the current list of local users, and it allows you to add or remove local users. The list of local users entered here is used when configuring user-based rules, such as Attachment Checking rules and Content Checking rules.

To add a new local user follow these steps:

1. Enter the email address in the **Email address** box.
2. Click **Add**.

NOTE: GFI MailSecurity uses the local domains list, configurable from the **Local Domains** tab, to determine whether a new email address is local or not. A notification dialog box is displayed if you enter a non-local user, as shown in the screenshot below.



Screenshot 38 - Non-local user entered

3. Repeat steps 1 and 2 to add more than one local user.
4. Click **Apply**.

To remove a local user follow these steps:

1. Select the local user you want to remove from the **Local Users** list.
2. Click **Remove**.
3. Repeat steps 1 and 2 to remove more than one local user.
4. Click **Apply**.

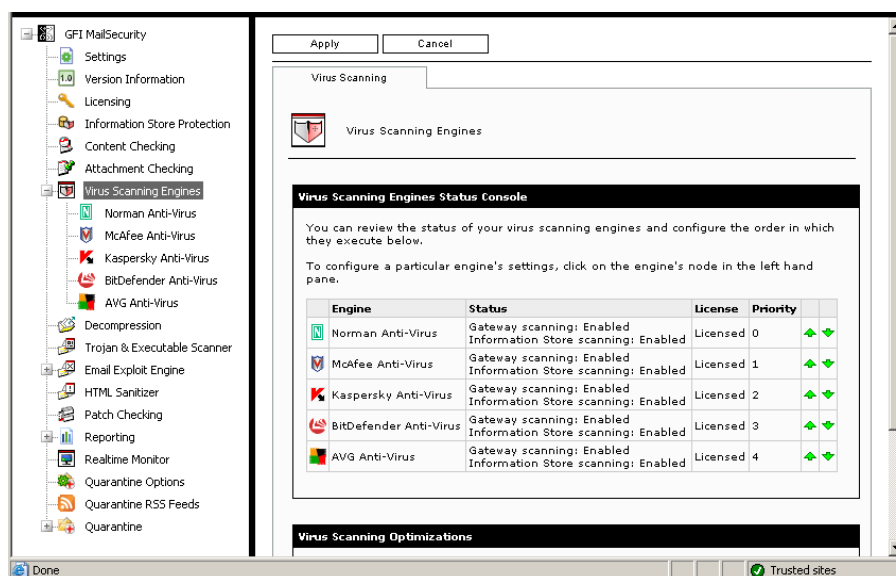
Configuring virus checking

Configuring Virus Scanning Engines

The virus-checking feature of GFI MailSecurity scans all SMTP traffic, inbound and outbound emails, for viruses using multiple Virus Scanning Engines. When GFI MailSecurity is installed on the Microsoft Exchange server machine, you can also configure GFI MailSecurity to scan the information store for viruses.

NOTE: When GFI MailSecurity is installed on a Microsoft Exchange Server 2007 machine, **Information Store Protection** is available only when the Mailbox Server Role and Hub Transport Server Role are installed.

GFI MailSecurity ships with both Norman and BitDefender Virus Scanning Engine as standard. However, you can optionally license the AVG, Kaspersky and McAfee Virus Scanning Engines, which are supported as well. All of the aforementioned anti-virus packages are proven and reliable virus detection engines, which have received many awards and certifications, including the industry leading certifications of ICSA.



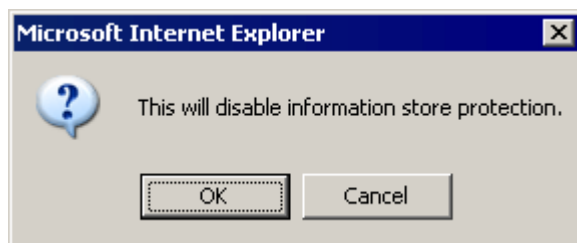
Screenshot 39 - Virus Scanning Engines status page

You can view the operational and license status of each Virus Scanning Engine along with the execution sequence of the installed Virus Scanning Engines by clicking on the **GFI MailSecurity ► Virus Scanning Engines** node.

The Virus Scanning Engines are listed in the same order of priority used by GFI MailSecurity to scan emails for viruses (Priority 0 being the highest or top priority).

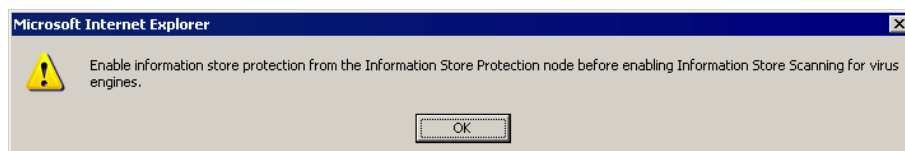
Each Virus Scanning Engine must be configured separately. To configure virus checking, click the required Virus Scanning Engine from the Status page on display in the right window. Alternatively, you can expand the **Virus Scanning Engines** node and click the required Virus Scanning Engine node (for example, Kaspersky).

NOTE: If you are running GFI MailSecurity on a Microsoft Exchange machine and the **Information Store Scanning** status is set to **Disabled** for all Virus Scanning Engines, the Information Store Scanning feature is disabled. The GFI MailSecurity configuration will inform you with a dialog that the Information Store Scanning feature is going to be disabled since you are trying to disable the only Virus Scanning Engine left which is set to scan the Information Store. If you click **OK**, the particular virus-scanning engine will have the Information Store Scanning feature disabled and so will the overall Information Store Scanning feature. If you click **Cancel**, the virus-scanning engine will not have the Information Store Scanning feature disabled and the overall Information Store Scanning feature will remain active since there is at least one virus-scanning engine that is still configured to scan the Information Store.



Screenshot 40 – Information Store Scanning will be disabled.

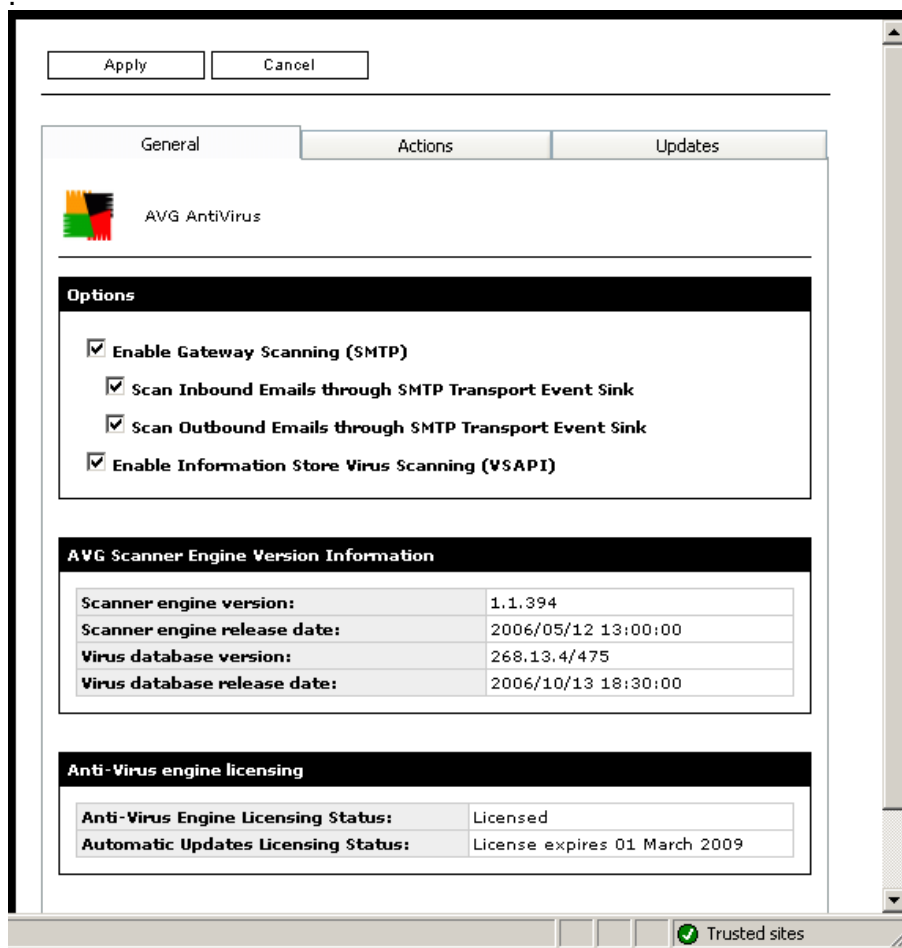
If the overall Information Store Scanning feature is disabled, you need to enable it from the **Information Store Protection** node before you can configure any Virus Scanning Engine to scan the Information Store. If you try to configure a Virus Scanning Engine to scan the Information Store and the feature is disabled from the **Information Store Protection** node, the GFI MailSecurity configuration will inform you about this with a dialog as shown in the screenshot below.



Screenshot 41 – Enable Information Store protection before configuring a Virus Scanning Engine

AVG configuration

NOTE: The AVG virus engine must be purchased separately: This engine is not included in the base product. As standard, GFI MailSecurity includes both the Norman and the BitDefender anti-virus engines. For pricing information on adding the AVG anti-virus engine, please visit the GFI website (www.gfi.com).



Screenshot 42 - Anti-virus Scanning Engines: AVG configuration page (General Tab)

To configure the AVG engine:

1. Expand the **GFI MailSecurity ► Virus Scanning Engines** node and then click **AVG**.
2. To scan SMTP traffic using this Virus Scanning Engine, select the **Enable Gateway Scanning (SMTP)** check box. You now need to select whether you want to scan inbound and outbound emails using this Virus Scanning Engine. To scan inbound emails select the **Scan Inbound Emails through SMTP Transport Event Sink** check box. To scan outbound emails select the **Scan Outbound Emails through SMTP Transport Event Sink** check box.
3. If you installed GFI MailSecurity on the Microsoft Exchange machine, you will also have the option to scan the Information Store using this Virus Scanning Engine. To scan the Information Store select the **Enable Information Store Virus Scanning (VSAPI)** check box.

NOTE: When GFI MailSecurity is installed on a Microsoft Exchange Server 2007 machine, information store scanning is available only when the Mailbox Server Role and Hub Transport Server Role are installed.

4. The configuration settings required in the **Actions** and **Updates** tabs are identical for all the installed virus-scanning engines. For more information on how to configure these parameters, refer to the 'Virus scanner actions' and 'Virus scanner updates' sections in this chapter.

5. After you have configured all the required parameters, click **Apply**. All changes and configuration settings will take effect immediately.

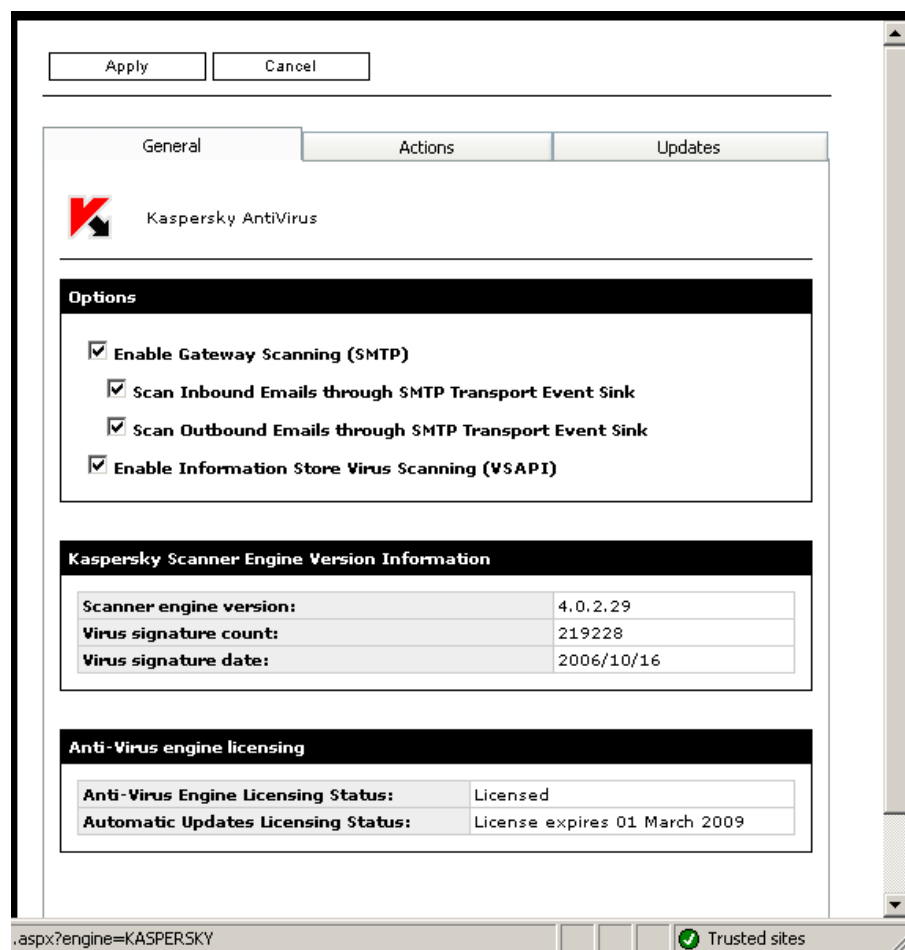
NOTE: The section at the bottom of the General tab displays information on the scanning engine. This includes the Virus database version and release date. License details for the current anti-virus engine are also displayed.

AVG web site

For more information about the virus patterns included in the AVG engine, visit the AVG website at <http://www.grisoft.com>.

Kaspersky configuration

NOTE: The Kaspersky virus engine must be purchased separately: This engine is not included in the base product. As standard, GFI MailSecurity includes both the Norman and the BitDefender anti-virus engines. For pricing information on adding the Kaspersky anti-virus engine, please visit the GFI website (www.gfi.com).



Screenshot 43 - Anti-virus Scanning Engines: Kaspersky configuration page (General Tab)

To configure the Kaspersky engine:

1. Expand the **GFI MailSecurity ► Virus Scanning Engines** node and then click **Kaspersky**.
2. To scan SMTP traffic using this Virus Scanning Engine, select the **Enable Gateway Scanning (SMTP)** check box. You now need to

select whether you want to scan inbound and outbound emails using this Virus Scanning Engine. To scan inbound emails select the **Scan Inbound Emails through SMTP Transport Event Sink** check box. To scan outbound emails select the **Scan Outbound Emails through SMTP Transport Event Sink** check box.

3. If you installed GFI MailSecurity on the Microsoft Exchange machine, you will also have the option to scan the Information Store using this Virus Scanning Engine. To scan the Information Store select the **Enable Information Store Virus Scanning (VSAPI)** check box.

NOTE: When GFI MailSecurity is installed on a Microsoft Exchange Server 2007 machine, information store scanning is available only when the Mailbox Server Role and Hub Transport Server Role are installed.

4. The configuration settings required in the **Actions** and **Updates** tabs are identical for all the installed Virus Scanning Engines. For more information on how to configure these parameters, refer to the 'Virus scanner actions' and 'Virus scanner updates' sections in this chapter.

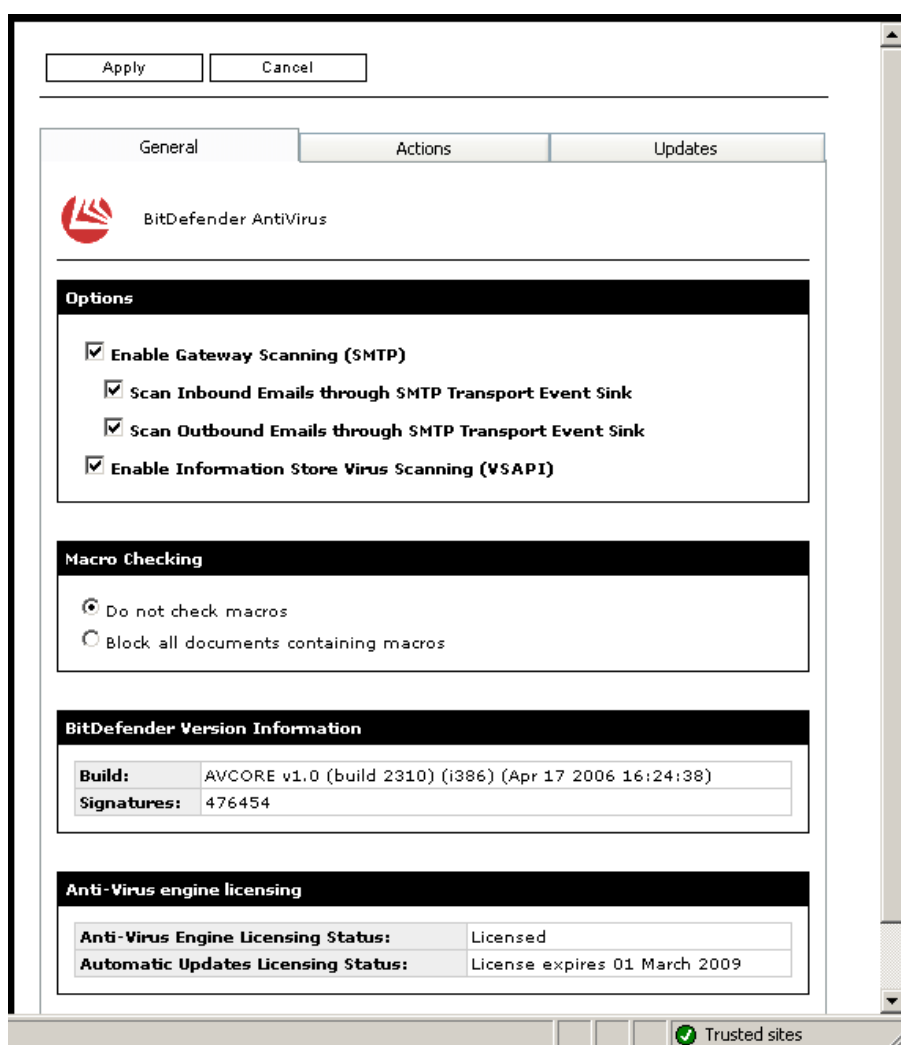
5. After you have configured all the required parameters, click **Apply**. All changes and configuration settings will take effect immediately.

NOTE: The section at the bottom of the General tab displays information on the scanning engine. This includes the Virus Scanning Engine version, virus signature count and the date of the current virus signature files. License details for the current anti-virus engine are also displayed.

Kaspersky web site

For more information about the virus patterns included in the Kaspersky engine, visit the Kaspersky website at <http://www.kaspersky.com>.

BitDefender configuration



Screenshot 44 - Virus Scanning Engines: BitDefender configuration page (General Tab)

To configure the BitDefender engine:

1. Expand the **GFI MailSecurity ► Virus Scanning Engines** node and then click **BitDefender**.
2. To scan SMTP traffic using this Virus Scanning Engine, select the **Enable Gateway Scanning (SMTP)** check box. You now need to select whether you want to scan inbound and outbound emails using this Virus Scanning Engine. To scan inbound emails select the **Scan Inbound Emails through SMTP Transport Event Sink** check box. To scan outbound emails select the **Scan Outbound Emails through SMTP Transport Event Sink** check box.
3. If you installed GFI MailSecurity on the Microsoft Exchange machine, you will also have the option to scan the Information Store using this Virus Scanning Engine. To scan the Information Store select the **Enable Information Store Virus Scanning (VSAPI)** check box.

NOTE: When GFI MailSecurity is installed on a Microsoft Exchange Server 2007 machine, information store scanning is available only when the Mailbox Server Role and Hub Transport Server Role are installed.

4. BitDefender Control also allows you to block or ignore emails with attachments that contain macros. This feature can be configured by selecting one of the following options:

- **Do not check macros** – Select this option if you want GFI MailSecurity to ignore macros and only scan emails for viruses.
- **Block all documents containing macros** – Select this option if you want to quarantine all emails that contain a macro (even if the macro is a genuine one).

NOTE: Quarantining of emails depends on the Actions configured in the Virus Scanning Engine. If you select **Delete item** in the **Actions** tab of the Antivirus Engine, all emails containing macros will still be DELETED (i.e. they are NOT Quarantined).

5. The configuration settings required in the Actions and Updates tabs are identical for all the installed Virus Scanning Engines. For more information on how to configure these parameters, refer to the 'Virus Scanner Actions' section and 'Virus Scanner Updates' section in this chapter.

6. After you have configured all the required parameters, click **Apply**. All changes and configuration settings will take effect immediately.

NOTE: The section at the bottom of the General tab displays information on the scanning engine. This includes the Virus Scanning Engine version and the virus signature count. License details for the current anti-virus engine are also displayed.

BitDefender website

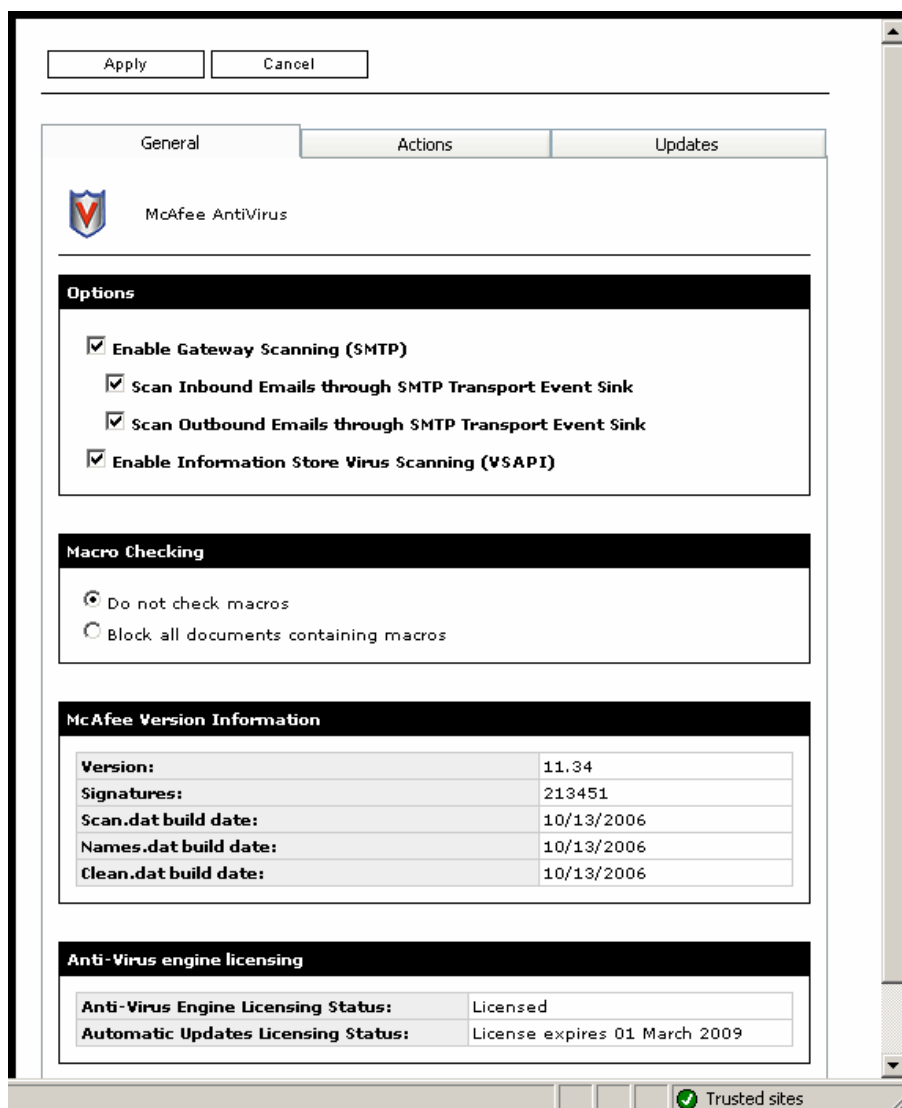
For more information about the virus patterns included in the BitDefender engine, visit the BitDefender website at <http://www.bitdefender.com>

McAfee configuration

NOTE: The McAfee engine is purchased separately: the engine is not included in the base product. As standard, GFI MailSecurity includes both the Norman and the BitDefender anti-virus engine. For pricing information on adding the MacAfee anti-virus engine, please visit the GFI website (www.gfi.com).

The configuration options of the McAfee Virus Scanning Engine are identical to those of the BitDefender engine. For more information on how to configure these options, refer to the 'BitDefender Configuration' section earlier in the manual.

NOTE: The section at the bottom of the General tab displays information on the scanning engine. This includes the Virus Scanning Engine version, virus signature count and the date of the current virus signature files. License details for the current anti-virus engine are also displayed.



Screenshot 45 - Virus Scanning Engines: McAfee configuration page (General Tab)

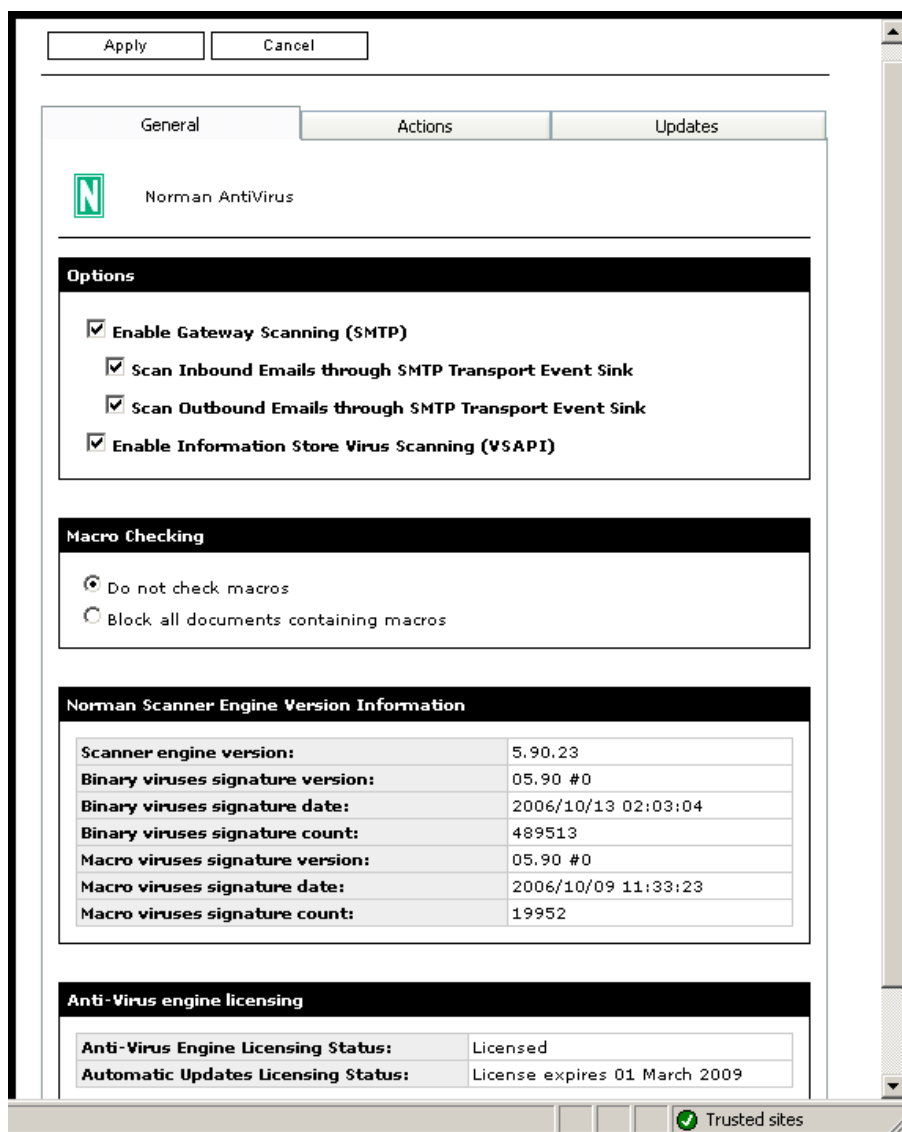
McAfee website

For more information about the virus patterns included in the McAfee engine, visit the McAfee website at <http://www.mcafee.com>

Norman configuration

The configuration options of the Norman Virus Scanning Engine are identical to those of the BitDefender engine. For more information on how to configure these options, refer to the 'BitDefender Configuration' section earlier in the manual.

NOTE: The section at the bottom of the General tab displays information on the scanning engine. This includes the Virus Scanning Engine version, virus signature count and the date of the current virus signature files. License details for the current anti-virus engine are also displayed.

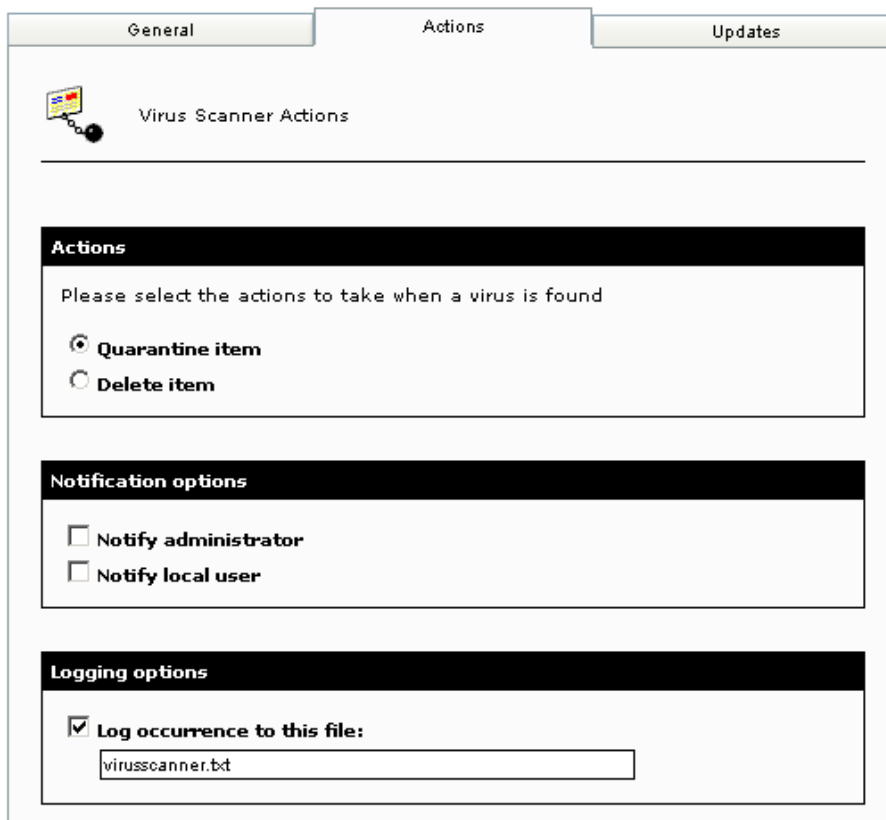


Screenshot 46 - Virus Scanning Engines: Norman configuration page

Norman website

For more information about the virus patterns included in the Norman Virus Control (NVC) engine, visit the NVC website at <http://www.norman.com>

Virus scanner actions



The screenshot shows the 'Virus Scanner Actions' configuration window. It has three tabs: 'General', 'Actions' (which is active), and 'Updates'. Below the tabs is a header area with a small icon and the text 'Virus Scanner Actions'. The main content area is divided into three sections, each with a black header bar. The first section, 'Actions', contains the instruction 'Please select the actions to take when a virus is found' and two radio button options: 'Quarantine item' (which is selected) and 'Delete item'. The second section, 'Notification options', contains two unchecked checkboxes: 'Notify administrator' and 'Notify local user'. The third section, 'Logging options', contains a checked checkbox for 'Log occurrence to this file:' followed by a text input field containing the filename 'virusscanner.txt'.

Screenshot 47 - Virus Scanning Engine: Configuration page (Actions Tab)

In GFI MailSecurity, you can configure what each of the installed Virus Scanning Engines should do whenever an infected email is detected. To configure the actions of a virus scanner:

1. Select the virus scanner that you want to configure and click the **Actions** tab.
2. Choose one of the following options:
 - **Quarantine item** – Select this option if you want to quarantine all virus-infected emails detected by this Virus Scanning Engine. You can subsequently review (approve/delete) all the quarantined emails.
 - **Delete item** – Select this option to delete all virus-infected emails detected by this Virus Scanning Engine.

NOTE: This option overrides the settings configured in the **General** tab. i.e. If in the **General** tab, you selected **Block all emails containing a macro** (i.e. quarantine all emails even the ones having a genuine macro) but at the same time you have enabled the **Delete item** option, ALL emails containing a macro will be deleted.

3. To send email notifications whenever an infected email is detected, enable any of the following options:

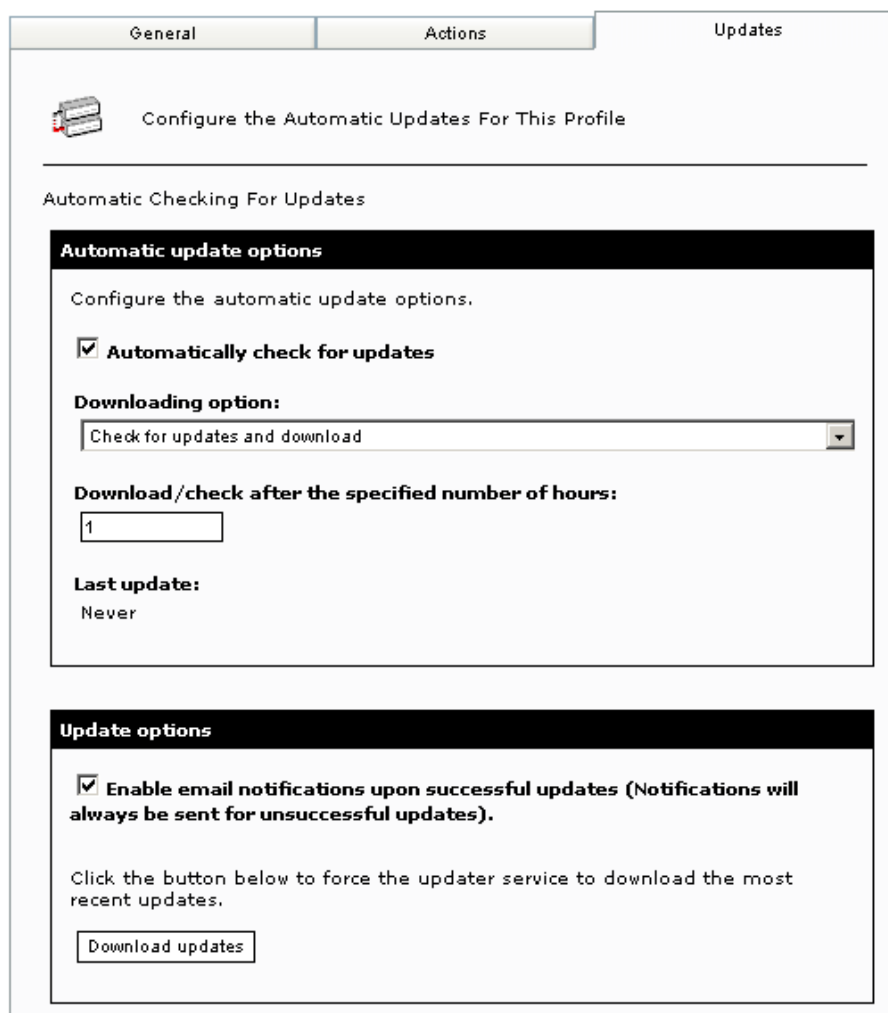
- **Notify local user** – Select this option if you want to notify the email local users when this filter detects a virus.

NOTE: If a threat is detected in an outbound email, the recipients will receive the original email with the malicious parts removed. A security notice is attached to the email to inform the recipients

what email parts were removed and for what reason. This behavior is always enabled and is not affected by this setting.

- **Notify administrator** – Select this option if you want to notify the administrator whenever this virus scanner detects an infected email.
4. Select the **Log occurrence to this file** check box and specify a log file name in the box below, if you want to log the virus scanning activity to a log file. You can specify either the file name only or else the full path to a custom location on disk.

Virus scanner updates



The screenshot displays the 'Updates' tab of the 'Virus Scanning Engines: Configuration' page. At the top, there are three tabs: 'General', 'Actions', and 'Updates', with 'Updates' being the active tab. Below the tabs is a header area with a server icon and the text 'Configure the Automatic Updates For This Profile'. The main content area is titled 'Automatic Checking For Updates' and contains two sections. The first section, 'Automatic update options', has a sub-header 'Configure the automatic update options.' and includes a checked checkbox for 'Automatically check for updates'. Below this is a 'Downloading option:' dropdown menu set to 'Check for updates and download'. Further down is a 'Download /check after the specified number of hours:' field with the value '1'. The 'Last update:' status is shown as 'Never'. The second section, 'Update options', has a checked checkbox for 'Enable email notifications upon successful updates (Notifications will always be sent for unsuccessful updates)'. Below this is a text prompt 'Click the button below to force the updater service to download the most recent updates.' and a 'Download updates' button.

Screenshot 48 - Virus Scanning Engines: Configuration page (Updates Tab)

You can configure GFI MailSecurity to download virus scanner updates automatically or to notify the administrator whenever new updates are available. To configure the automatic updates of a particular virus scanner:

1. Select the virus scanner that you want to configure and from the right window, click the **Updates** tab.
2. Select the **Automatically check for updates** check box to enable the auto-update feature.
3. From the **Downloading options** list, select one of the following:

- **Only check for updates** – Select this option if you want GFI MailSecurity to just check and notify the administrator whenever updates are available for this virus scanner.

NOTE: This option will NOT download the available updates.

- **Check for updates and download** – Select this option if you want GFI MailSecurity to check and automatically download any updates available for this virus scanner.

4. Specify how often you want GFI MailSecurity to check/download updates for this Virus Scanning Engine, by specifying an interval value in hours.






Triggering the virus update manually

To check/download updates for the current Virus Scanning Engine immediately, click **Download updates**.

Setting the Virus Scanning Engines scan priority

To configure the execution order of the Virus Scanning Engines, follow these steps:

1. Click the **GFI MailSecurity ► Virus Scanning Engines** node.

Engine	Status	License	Priority		
 AVG Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	0	▲	▼
 BitDefender Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	1	▲	▼
 Norman Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	2	▲	▼
 McAfee Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	3	▲	▼
 Kaspersky Anti-Virus	Gateway scanning: Enabled Information Store scanning: Enabled	Licensed	4	▲	▼

Screenshot 49 - Virus Scanning Engines: scan priority list

2. In the right pane, the Virus Scanning Engines are listed in descending order of priority.

NOTE: The priority assigned to each virus scanner determines the sequence when each anti-virus engine gets to scan the content. The scanner with priority 0 is the first to start scanning an email. Upon completion, the Virus Scanning Engine with priority 1 scans the email and so on. This means that the Virus Scanning Engine listed at the top of the list is the first to scan emails, if it is enabled.

3. To change the virus scanning execution priority, click the (up) ▲ or (down) ▼ arrows to respectively increase or decrease the priority of the virus scanner. Repeat the same procedure until the virus scanner reaches the desired position in the priority/execution sequence list.

Configuring Virus Scanning optimizations

From the **GFI MailSecurity ► Virus Scanning Engines** node you can instruct GFI MailSecurity to stop virus scanning an item if a number of virus scanning engines already detected a virus in that item.

To enable this option, select the **Stop virus scanning the current item, if viruses are detected by** check box, and specify the number

of virus scanners that need to detect a virus to stop virus scanning, in the box. Click **Apply**.

Virus Scanning Optimizations

☒ Stop virus scanning the current item, if viruses are detected by:
 virus scanners

☒ Stop scanning even for non-virus related threats.

Screenshot 50 - Configure virus scanning optimizations

For example, if you select this option and enter 2 in the box, virus scanning on an item that contains a virus is performed by at most two virus-scanning engines, if they detect it. Emails that do not contain a virus are scanned by all enabled virus-scanning engines anyway.

If you want to streamline further the path taken by items containing a virus, select the **Stop scanning even for non-virus related threats** check box and click **Apply**. This option will instruct GFI MailSecurity to stop further scanning of the current item, such as with Attachment Checking and so on, since the amount of virus-scanning engines you specified have detected a virus.

Configuring Information Store Scanning

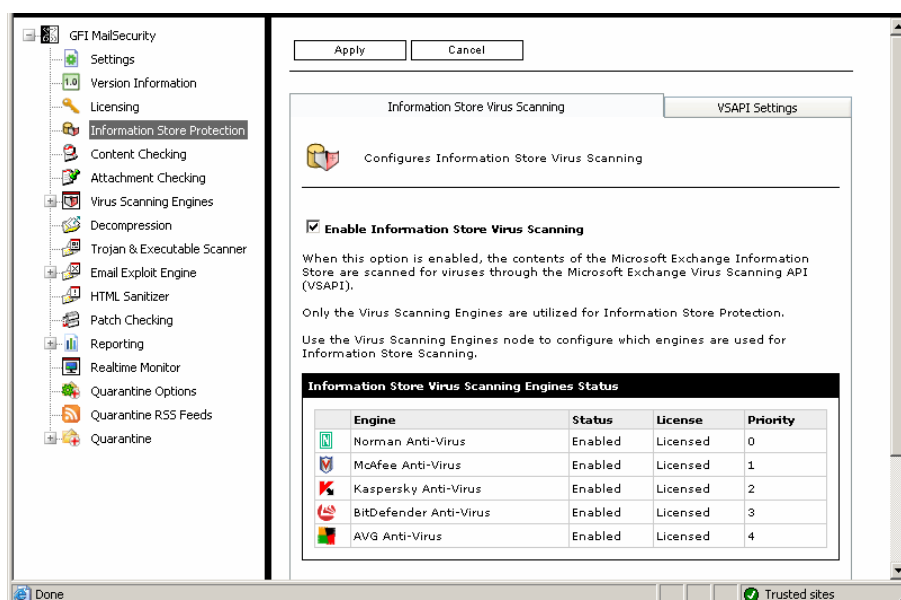
NOTE 1: The **Information Store Protection** node is only available if you install GFI MailSecurity on the Microsoft Exchange machine.

NOTE 2: When GFI MailSecurity is installed on a Microsoft Exchange Server 2007 machine, **Information Store Protection** is available only when the Mailbox Server Role and Hub Transport Server Role are installed.

This section will show you how to enable or disable Information Store Scanning, and select the scan method used by VSAPI (Virus Scanning API).

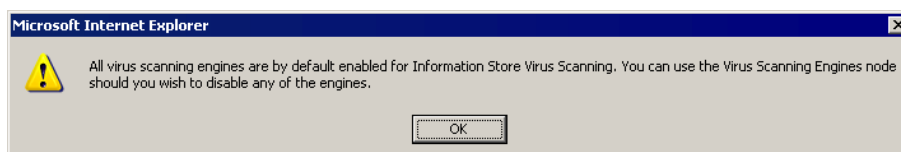
To configure the Information Store Scanning feature, follow these steps:

1. Click the **GFI MailSecurity ► Information Store Protection** node.
2. In the **Information Store Virus Scanning** tab, you can enable or disable Information Store Scanning by selecting/clearing the **Enable Information Store Virus Scanning** check box accordingly. The status of the Virus Scanning Engines used to scan the Information Store is also displayed.



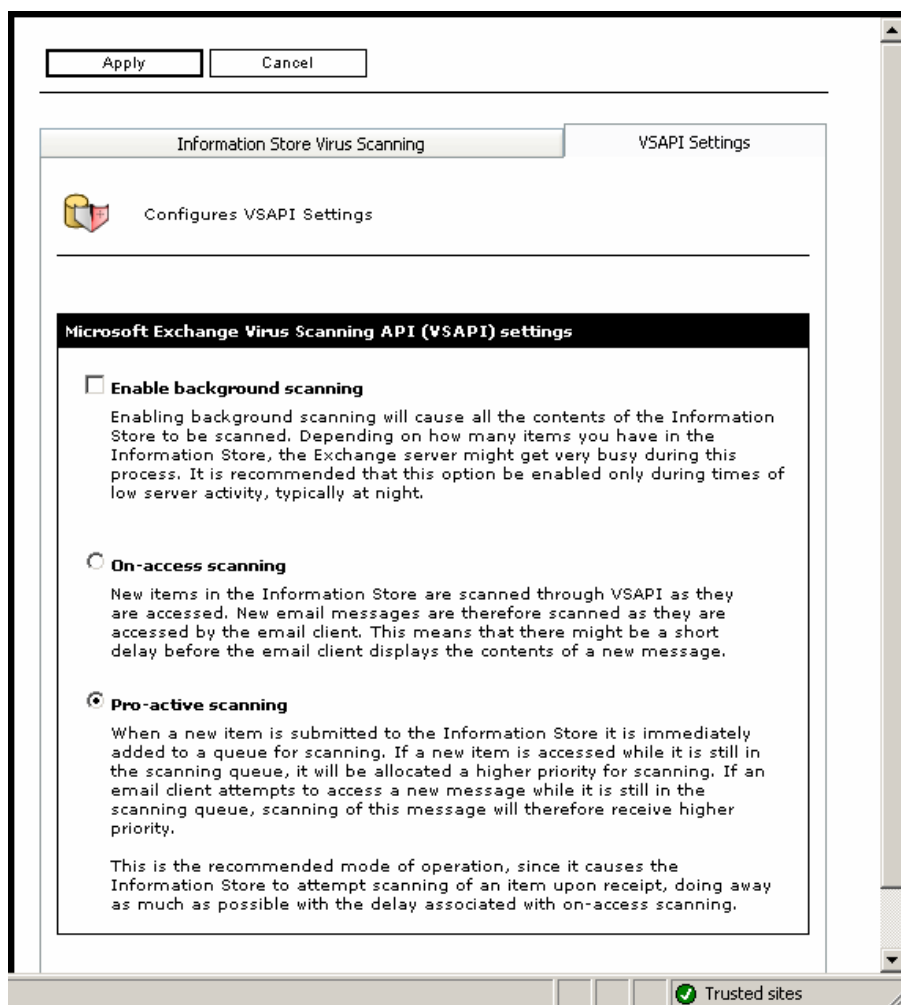
Screenshot 51 – Information Store Protection node

NOTE: When you disable Information Store Virus Scanning, the Information Store Scanning option of all Virus Scanning Engines is disabled automatically. When you enable Information Store Virus Scanning, the Information Store Scanning option of all Virus Scanning Engines is enabled automatically. This setting does not affect the Gateway scanning option of each Virus Scanning Engine. The GFI MailSecurity configuration will prompt you about this action as shown in the screenshot below. If you need to enable or disable the Information Store Scanning option for a specific Virus Scanning Engine, please refer to the 'Configuring Virus Scanning Engines' section earlier in this chapter.



Screenshot 52 – All Information Store Virus Scanning Engines have been enabled.

3. To configure what VSAPI scan method to use, click the **VSAPI Settings** tab.



Screenshot 53 – VSAPI scan settings

4. From the VSAPI Settings tab, you can enable background Information Store Scanning, by selecting the **Enable background scanning** check box. This option will cause all the contents of the Information Store to be scanned, which depending on the amount of items stored in the Information Store could result in a huge processing load on the Exchange server. For this reason, it is recommended that this option be only enabled during periods of low server activity such as during the night.

5. Select a VSAPI scan method from the following:

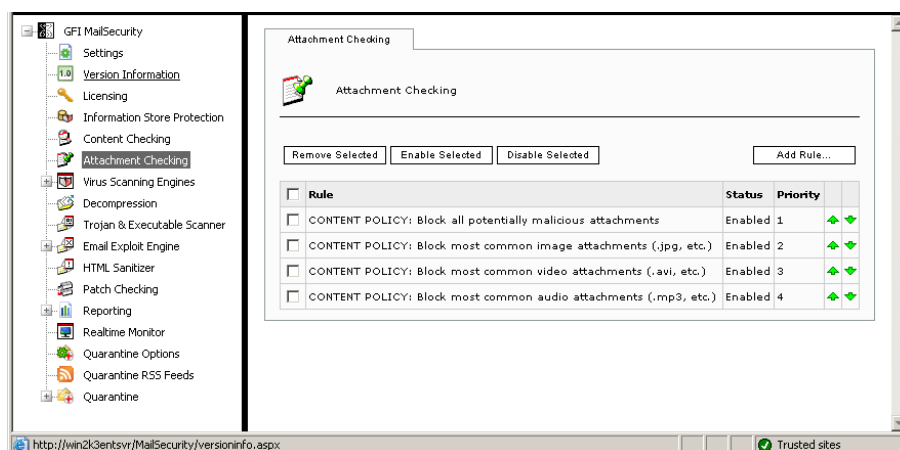
- **On-access scanning** – New items in the Information Store are scanned as soon as they are accessed by the email client. This scan method will thus introduce a short delay before the email client can display the contents of a new message.
- **Pro-active scanning** – New items added to the Information Store are added to a queue for scanning. When a mail client tries to access an item that is still in the queue, it will be allocated a higher scanning priority so that it is scanned as soon as possible. This is the default and recommended mode of operation, since in general the delay associated with on-access scanning is avoided because new items are added to the queue immediately and are usually scanned before a mail client requests access to the item.

6. To save and instruct GFI MailSecurity to make use of the new settings, click **Apply**.

Configuring Attachment Checking

Introduction to Attachment Checking

This chapter explains how to set up Attachment Checking in GFI MailSecurity. The Attachment Checking feature allows you to set up a policy regarding what types of email attachments you will allow on your mail server. To set up such a policy, GFI MailSecurity uses the concept of 'Rules'. A rule is a condition that you set, such as, “block all executable attachments”. This means that an Attachment Checking rule allows you to block attachments of a certain type.



Screenshot 54 - Attachment Checking page

In GFI MailSecurity, you can configure attachment rules from the **Attachment Checking** node. This page contains the options that enable you to create, delete, enable or disable rules. In addition, it lists all the existing attachment rules, including their status and the order in which these rules are applied to emails (i.e. priority).

Creating an Attachment Checking rule

To create an Attachment Checking rule:

1. Click the **GFI MailSecurity ► Attachment Checking** node.
2. From the Attachment Checking page (in the right window), click **Add Rule**.

General
Actions
Users/Folders

Attachment Checking

Rule display name

Rule name:

Email checking

☒ Check inbound emails

☒ Check outbound emails

Attachment blocking

☐ Block all

☒ Block this list

☐ Block all except this list

Enter filenames with optional wildcards:
 (eg. *.vbs)
 (eg. *letter.vbs)
 (eg. happy*.exe)
 (eg. orders.mdb)

Options

☐ Block all files greater than the following size in Kb:

Screenshot 55 - Attachment Checking: General Tab

3. Specify the name of the rule and select whether to apply this rule to inbound and/or outbound emails by selecting the respective check boxes.
4. Decide on the type of attachment blocking required:
 - **Block all** – Select this option to block email attachments of any type.
 - **Block this list** – Select this option to block ONLY the listed attachment types.

- **Block all except this list** - Select this option to block attachment types that are not included in the list.

NOTE 1: To add an attachment type to the list, input the required full file name or file extension in the box next to the **Add** button. When ready, click **Add**. You can use asterisk (*) wildcards to replace characters or strings in the attachment type/extension. For example, specifying **orders*.mdb* blocks all mdb files which contain the string 'orders' in the file name. Specifying **.jpg* will block all jpg files.

NOTE 2: To remove an entry from the list, select it and click **Remove Selected**.

5. Additionally, you can specify a file size in kilobytes as a threshold. This has the effect of blocking all attachments with a file size bigger than the one you specify irrespective of whether it matches an entry in the list. To enable this option, select the **Block all files greater than the following size in Kb** check box and specify the maximum file size (in KB) allowed without blocking.

The screenshot shows the 'Attachment Checking Actions' configuration window. It has three tabs: 'General', 'Actions', and 'Users/Folders'. The 'Actions' tab is active. The window title is 'Attachment Checking Actions'. Below the title bar, there are three main sections: 'Actions', 'Notification options', and 'Logging options'. In the 'Actions' section, the checkbox 'Block attachment and perform this action:' is checked. Below it, there are three radio button options: 'Quarantine email' (selected), 'Delete email', and 'Move to folder:' (with an empty text input field). In the 'Notification options' section, both 'Notify administrator' and 'Notify local user' are checked. In the 'Logging options' section, 'Log rule occurrence to this file:' is checked, and the text input field below it contains 'attachmentchecking.txt'.

Screenshot 56 - Attachment Checking: Actions Tab

6. After you have specified what the attachment rule should check for, you must specify what this rule should do whenever it finds the specified attachment(s). Click the **Actions** tab to open the rule actions configuration page.

7. Select the **Block attachment and perform this action** check box if you want to quarantine, delete or move the blocked emails to a particular folder. Additionally, select one of the following options:

- **Quarantine email:** Select this option to quarantine the email containing the attachment for review by an administrator. For more information, refer to the 'Quarantining' chapter in this manual.

- **Delete email:** Select this option to delete the email and attachment completely.
- **Move to folder:** This option will move the email to the specified folder. Input the folder name in the box provided underneath this option.

NOTE: Please note that you cannot configure actions to affect a single attachment within an email. Actions will always affect the whole email containing the attachment.

8. You can configure an attachment rule to send email notifications to the administrator and/or user whenever an email containing an attachment is blocked. You can configure the required notifications by selecting any of the following options:

- **Notify local user:** Select this option if you want to notify the email local users when this filter blocks an attachment.

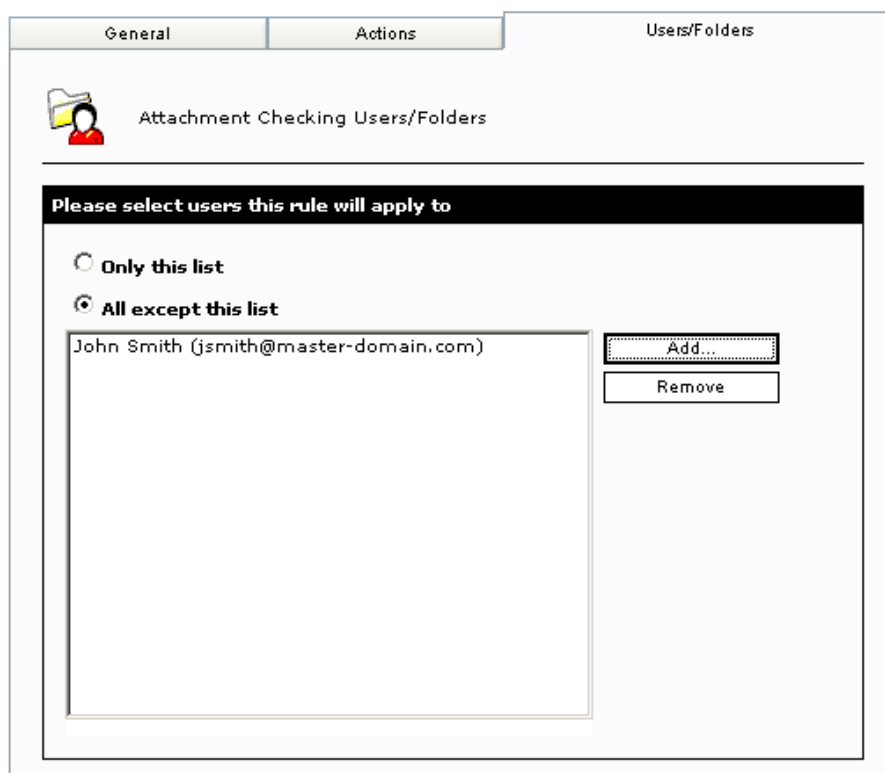
NOTE: If a threat is detected in an outbound email, the recipients will receive the original email with the malicious parts removed. A security notice is attached to the email to inform the recipients what email parts were removed and for what reason. This behavior is always enabled and is not affected by this setting.

- **Notify administrator:** Select this option if you want to send email notifications to the administrator whenever an email containing an attachment is blocked. The administrator's email address is specified during the installation of GFI MailSecurity but can still be changed from the GFI MailSecurity configuration (**GFI MailSecurity** ► **Settings** node ► **General** tab). For more information refer to the 'Define the administrator's email address' section in the General Settings chapter.

9. Select the **Log rule occurrence to this file** check box and specify a log file name in the box below, if you want to log all rule activity to a log file. You can specify either the file name only or else the full path to a custom location on disk.

NOTE: You can configure an attachment rule using any combination of actions. For example, you can opt not to block emails containing the attachment, but to simply notify the user or log the occurrence to file.

10. Now, you must specify the users to whom this rule applies. By default, GFI MailSecurity will apply the rule to all email users. However, if you want this rule to affect a selection of users only, click the **Users/Folders** tab.

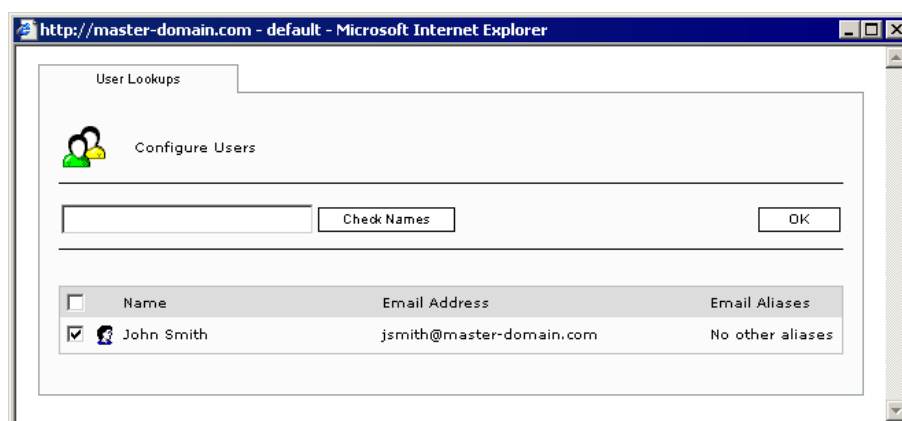


Screenshot 57 - Attachment Checking: Users/Folders Tab

11. Choose one of the following options:

- **Only this list** – Select this option if you want to apply this rule to all email users/groups or public folders present in the list.
- **All except this list** – Select this option if you want to apply this rule to all email users, groups or public folders NOT present in the list.

12. To add email users, user groups and/or public folders to the list, click **Add**.



Screenshot 58 - Add users to an attachment checking rule

13. In the add users window, specify the name of the email user/user group or public folder that you wish to add to the list.

14. Click **Check Names** to query the Active Directory or the imported list of SMTP addresses (depending on how you installed GFI MailSecurity), to check if the specified entry exists. Any user, group or public folder that matches will be listed below.

NOTE: You do not need to input the full name of the user/user group or public folder. It is enough to enter at least three characters. GFI MailSecurity will list all the names that contain the specified characters. For example, if you input 'ott', GFI MailSecurity will return names like 'Scott Adams' and 'Freeman Prescott', if they are available.

15. Select the check box at the start of the listed name(s) to indicate the ones that you wish to add to the list and click **OK**.

NOTE 1: You can select all the listed names at once by selecting the check box next to the **Name** column heading at the top-left of the list.

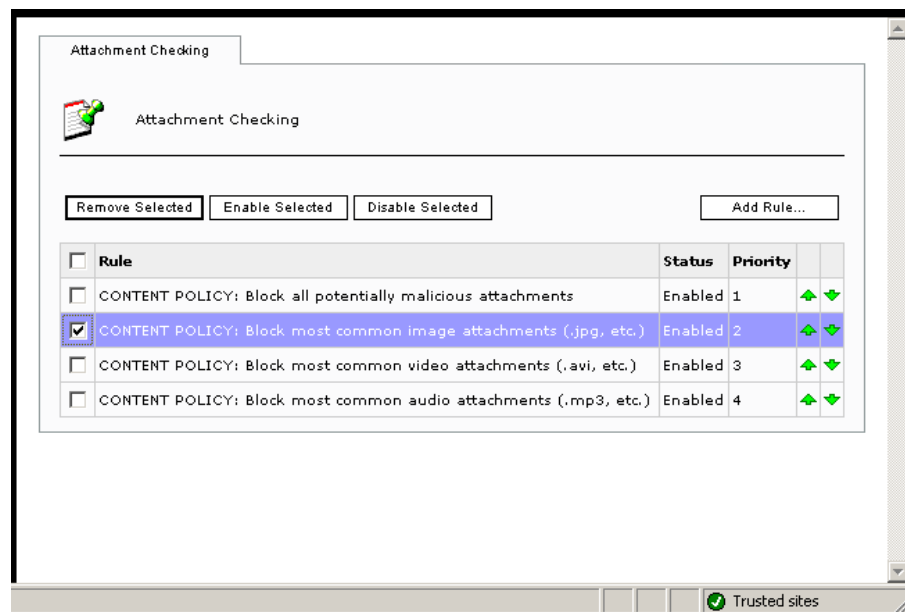
NOTE 2: Repeat steps 12 to 15 to add all the users you want to the list.

NOTE 3: To remove entries from the list, select the user/user group/public folder you want to remove and click **Remove**.

NOTE 4: If no names are included in the list, GFI MailSecurity will automatically apply this rule to all the email users in Active Directory/SMTP address list.

16. Click **Apply**.

Removing attachment rules



Screenshot 59 - Selecting an attachment checking rule for removal

To Remove an Attachment Checking rule:

1. Click the **GFI MailSecurity ► Attachment Checking** node.
2. From the Attachment Checking page (in the right window), select the check box of the rule(s) that you want to remove.

NOTE: You can select all check boxes in one go by selecting the check box next to the **Rule** column heading at the top-left of the list.

3. Click **Remove Selected** to delete the selected rules.

Make changes to an existing rule

To modify an existing rule:

1. Click the **GFI MailSecurity ► Attachment Checking** node.
2. From the Attachment Checking page (in the right window), click the name of the rule that you want to modify.
3. Make the required changes (for example, Rename the rule, etc.) in the rule properties and click **Apply** to accept the changes you made. Changes will take effect immediately.



Enabling/disabling rules

You can check and change the status of a rule (i.e. enabled/disabled) from the Attachment Checking page. To enable or disable an existing rule:

1. Click the **GFI MailSecurity ► Attachment Checking** node.
2. From the Attachment Checking page (in the right window), select the check box of the rule(s) that you want to enable or disable.
3. Click **Enable Selected** or **Disable Selected** accordingly. The status change is displayed immediately under the **Status** column.

Changing the rule priority

Attachment Checking rules are applied in the same order, from top to bottom, as they are listed in the Attachment Checking page. However, you can change the sequence/priority of a rule as follows:

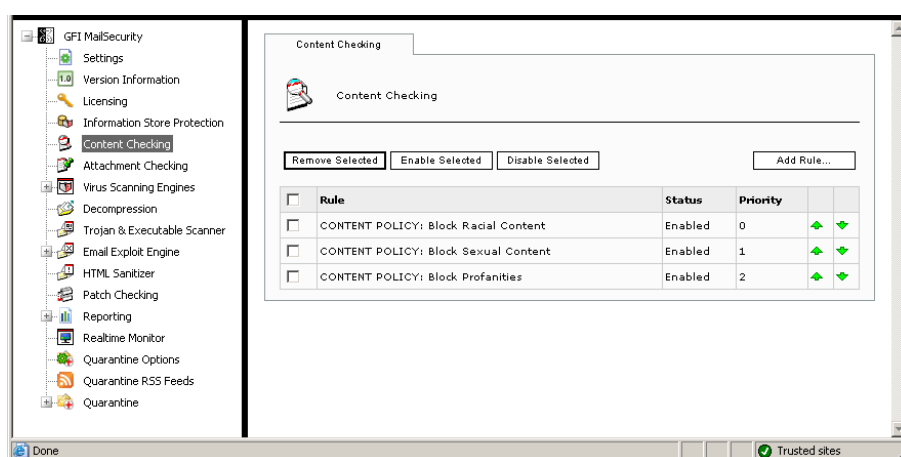
1. Click the **GFI MailSecurity ► Attachment Checking** node.
2. From the Attachment Checking page (in the right window), click the (up)  or (down)  arrows to respectively increase or decrease the priority of the required rule(s). Repeat until the rule reaches the desired position in the list (i.e. until the rule is assigned the desired priority).

NOTE: You can check the priority of rules from the Attachment Checking page. The priority value of each rule is displayed in the **Priority** column.

Configuring Content Checking

Introduction to Content Checking

This chapter will show you how to set up Content Checking in GFI MailSecurity. The Content Checking feature allows you to create rules in which you define keywords and logical operators to filter emails that contain offensive or confidential information for example.



Screenshot 60 - Content Checking page


In GFI MailSecurity, you can configure Content Checking rules from the **Content Checking** node. This page lists all the existing content checking rules, and it allows you to disable or enable them and set their processing priority. From this page, you can also create new content checking rules as well as delete and modify existing content checking rules.

Creating a Content Checking rule

To create a Content Checking rule:

1. Click the **GFI MailSecurity ► Content Checking** node.
2. From the Content Checking page (in the right window), click **Add Rule**.
3. In the **General** tab, enter the name for the new Content Checking rule. The rule name should ideally describe what content this rule blocks, so that you can easily distinguish rules if you have multiple Content Checking rules configured.
4. Select whether this rule applies to inbound and/or outbound emails by selecting the respective check boxes.

General Body Subject Actions Users/Folders

 Content Checking Options

Rule name

Please specify a friendly name for this rule:

Confidential Information Rule

Email checking

This rule can be applied to both inbound and outbound emails. Select below:

☒ Check inbound emails

☒ Check outbound emails

PGP Encryption

This rule can be set to block any PGP encrypted mail. Enable or disable this option below:

☐ Block PGP encrypted emails

Screenshot 61 - Content Checking: General Tab

5. If you want PGP encrypted emails to infringe this rule, select the **Block PGP encrypted emails** check box.

6. Next, you need to configure whether to scan email bodies and attachments, and the keywords an email must contain to trigger this Content Checking rule. Click the **Body** tab to configure these options.

7. To configure this rule to check email bodies you need to select the **Block emails if content is found matching these conditions (message body/attachments)** check box.

8. You then need to specify the conditions that will infringe this rule while scanning the bodies and attachments content. To enter a new condition, type the keywords in the **Edit condition** box. Click the required logical operator button to insert that operator at the current cursor location in the **Edit condition** box. When the condition is complete, click **Add Condition** to add the new condition to the rule. The new condition is then displayed in the **Current conditions** list.

For example to enter the following condition, “confidential information AND top secret”, you would perform the following steps:

In the **Edit condition** box, type “**confidential information**”.

Click **AND** to the right of the box.

Type “**top secret**” and click **Add Condition**.

NOTE: To remove a condition select it from the **Current conditions** list and click **Remove**. To modify an existing condition, select it from the **Current conditions** list to display it in the **Edit condition** box. Modify the condition as required and then click **Update** to save your changes.


General

Body

Subject

Actions

Users/Folders



Configure content checking options for checking the content of the message body and attachments.

☒ **Block emails if content is found matching these conditions (message body/attachments)**

Condition entry

Edit condition:

AND

OR

AND NOT

OR NOT

Add Condition

Update

Conditions list

All these conditions are validated as a single condition using the OR operator for each entry. Clicking on an entry will copy the condition text in the condition entry above for editing.

Current conditions:

confidential information AND top secret blueprints

Remove

Options

☒ **Match whole words only**
☒ **Apply above conditions to attachments**

Attachment filtering

☒ **Check all attachments having file extensions in this list**
☐ **Check all except attachments having file extensions in this list**

File extension entry:
(eg. txt)
(eg. jpg)

Add

File extensions:

txt
html
htm

Remove

Screenshot 62 - Content Checking: Body Tab

9. To match keywords in the conditions list only against whole words, select the **Match whole words only** check box.
10. If you want the Content Checking rule to scan email attachments for the conditions specified in the previous steps, select the **Apply above conditions to attachments** check box.
11. You then need to specify which filename extensions to scan. To add a filename extension, type it in the **File extension entry** box and then click **Add**. If you want to scan only the filename extensions you specify, click **Check all attachments having file extensions in the**

list. If you want to scan all the attachments except the ones you specified in the list, click **Check all except attachments having file extensions in the list.**

NOTE: Enter the filename extension only, for example, if you want to scan text files, enter “**txt**” only, not “***.txt**” or “**.txt**”.

12. If you want the Content Checking rule to check the email subject, click the **Subject** tab to specify the keywords that will infringe this rule if found in the email subject.

13. In the **Subject** tab, select the **Enable subject content checking** check box.

14. To add a keyword, type it in the **Enter phrase** box and then click **Add**. The new keyword is displayed in the **Phrases** list.

General Body Subject Actions Users/Folders

Content Checking Actions

☒ Enable subject content checking

Block emails with the following phrases in the 'Subject' field

Enter phrase:

Add

Phrases:

personal information

Remove Selected

Options

☐ Match whole words only

Screenshot 63 - Content Checking: Subject Tab

15. If you want to match only whole words, select the **Match whole words only** check box.

16. Next, configure what actions you want GFI MailSecurity to take on the emails that infringe this rule from the **Actions** tab.

17. Select the **Block email and perform this action** check box if you want to quarantine, delete or move the blocked emails to a particular folder. Additionally, select one of the following options:

Quarantine email: Select this option to quarantine the email containing the infringing content for review by an administrator. For more information, refer to the 'Quarantining' chapter in this manual.

Delete email: Select this option to delete the email completely.

Move to folder: This option will move the email to the specified folder. Type the folder name in the box provided underneath this option.

18. Content Checking rules can be configured to send email notifications to the administrator and/or user whenever an email infringes a rule. You can configure the required notifications by selecting any of the following options:

Notify local user: Select this option if you want to notify the email local users when the email infringes this content checking rule.

NOTE: If a threat is detected in an outbound email, the recipients will receive the original email with the malicious parts removed. A security notice is attached to the email to inform the recipients what email parts were removed and for what reason. This behavior is always enabled and is not affected by this setting.

Notify administrator: Select this option if you want to send email notifications to the administrator whenever an email infringes this content checking rule. The administrator's email address is specified during the installation of GFI MailSecurity but can still be changed from the GFI MailSecurity configuration (**GFI MailSecurity ► Settings** node ► **General** tab). For more information refer to the 'Define the administrator's email address' section in the General Settings chapter.

General Body Subject Actions Users/Folders

Content Checking Actions

Actions

☒ Block email and perform this action

☐ Quarantine email

☐ Delete email

☐ Move to folder:

Notification options

☒ Notify administrator

☒ Notify local user

Logging options

☒ Log rule occurrence to this file:

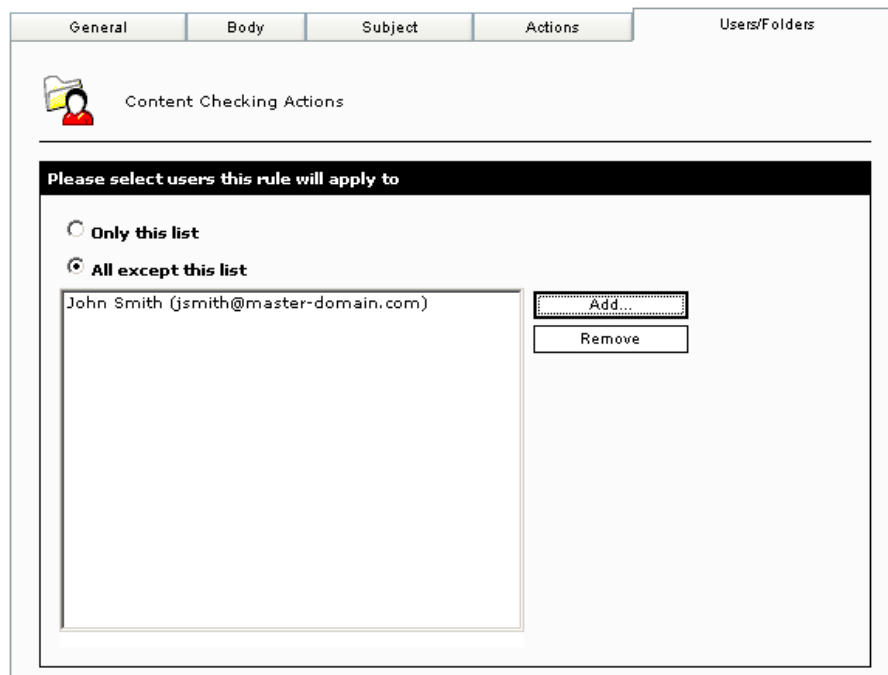
ConfidentialRuleInfringed.txt

Screenshot 64 - Content Checking: Actions Tab

19. Select the **Log rule occurrence to this file** check box and specify a log file name in the box below, if you want to log all rule activity to a log file. You can specify either the file name only or else the full path to a custom location on disk.

NOTE: You can configure a content checking rule using any combination of actions. For example, you can opt not to block emails infringing the rule, but to simply notify the administrator or log the occurrence to file.

20. Now, you must specify the users for whom this rule applies. By default, GFI MailSecurity will apply the rule to all email users. However, if you want this rule to affect only a selection of users, click the **Users/Folders** tab.



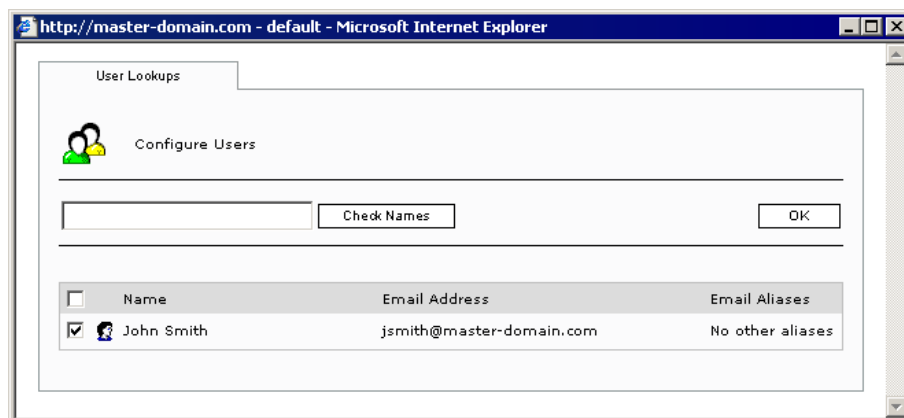
Screenshot 65 - Content Checking: Users/Folders Tab

21. Choose one of the following options:

Only this list – Select this option if you want to apply this rule to all email users/groups or public folders present in the list.

All except this list – Select this option if you want to apply this rule to all email users, groups or public folders NOT present in the list.

22. To add email users, user groups and/or public folders to the list, click the **Add** button.



Screenshot 66 - Add Users Dialog

23. In the add users window, specify the name of the email user/user group or public folder that you wish to add to the list.

24. Click **Check Names** to query the Active Directory or the imported list of SMTP addresses (depending on how you installed GFI

MailSecurity), to check if the specified entry exists. Any user, group or public folder that matches will be listed below.

NOTE: You do not need to input the full name of the user/user group or public folder. It is enough to enter at least three characters. GFI MailSecurity will list all the names that contain the specified characters. For example, if you input 'ott', GFI MailSecurity will return names like 'Scott Adams' and 'Freeman Prescott', if they are available.

25. Select the check box at the start of the listed name(s) to indicate the ones that you wish to add to the list and click **OK**.

NOTE 1: You can select all the listed names at once by selecting the check box next to the **Name** column heading at the top-left of the list.

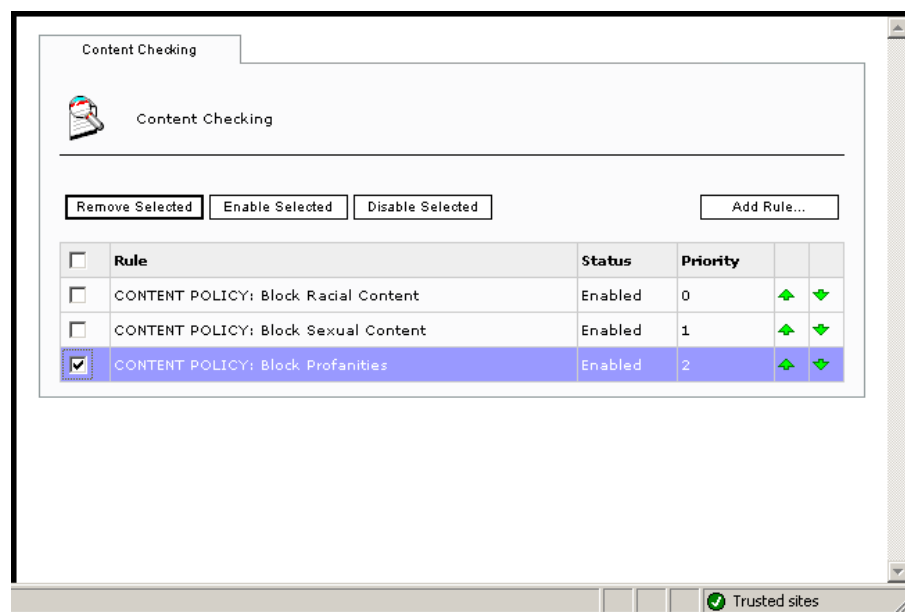
NOTE 2: Repeat steps 22 to 25 to add all the users you want to the list.

NOTE 3: To remove entries from the list, select the user/user group/public folder you want to remove and click **Remove**.

NOTE 4: If no names are included in the list, GFI MailSecurity will automatically apply this rule to all the email users in Active Directory/SMTP address list.

26. Click **Apply**.

Remove content checking rules



Screenshot 67 - Content Checking: Removing rules

To remove a Content Checking rule:

1. Click the **GFI MailSecurity ► Content Checking** node.
2. From the Content Checking page (in the right window), select the check boxes of the rules that you want to remove.

NOTE: You can select all check boxes in one go by selecting the check box next to the **Rule** column heading at the top-left of the list.

3. Click **Remove Selected** to delete the selected rules.

Make changes to an existing content checking rule

To modify an existing rule:

1. Click the **GFI MailSecurity ► Content Checking** node.
2. From the Content Checking page (in the right window), click the name of the rule that you want to modify. The content checking rule will be loaded.
3. Make the required changes (for example, rename the rule, etc.) in the rule properties and click **Apply**. Changes will take effect immediately.

Enabling/disabling rules

You can check and change the status of a rule (i.e. enabled/disabled) from the Content Checking page. To enable or disable an existing rule:



1. Click the **GFI MailSecurity ► Content Checking** node.
2. From the Content Checking page (in the right window), select the check box of the rule(s) that you want to enable or disable.
3. Click **Enable Selected** or **Disable Selected** accordingly. The status change is displayed immediately under the **Status** column.

Changing the rule priority

The content checking rule priority is used to determine what rule conditions should be checked for first and so on.

The Content Checking page lists the Content Checking rules in the same order as they will be checked, with the highest priority rule on top and the lowest priority rule at the end of the list. The priority number of each rule is displayed on the right hand side of the Content Checking page under the **Priority** column.

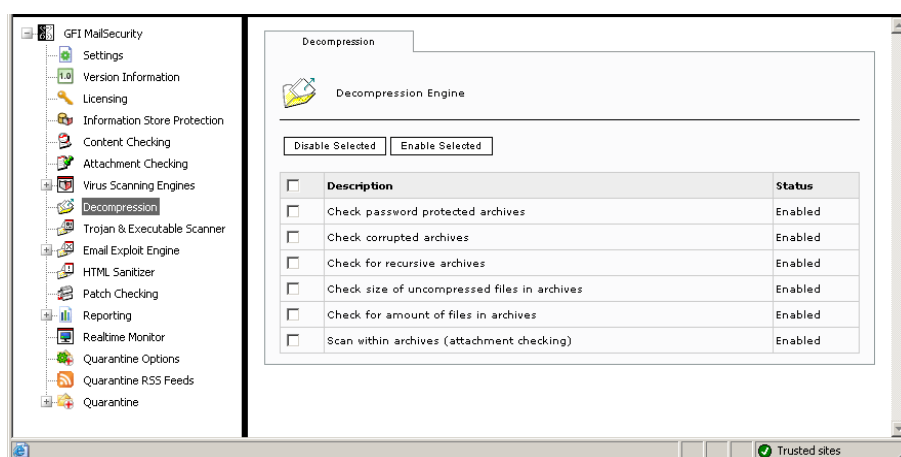
The Content Checking page allows you to change the priority of the rules as follows:

1. Click the **GFI MailSecurity ► Content Checking** node.
2. From the Content Checking page (in the right window), click the (up)  or (down)  arrows to respectively increase or decrease the priority of the required rule. Repeat until the rule reaches the desired position in the list (i.e. until the rule is assigned the desired priority).

Decompression engine

Introduction to the Decompression engine

The Decompression engine decompresses and analyzes archives attached to an email.



Screenshot 68 - The decompression engine filters list

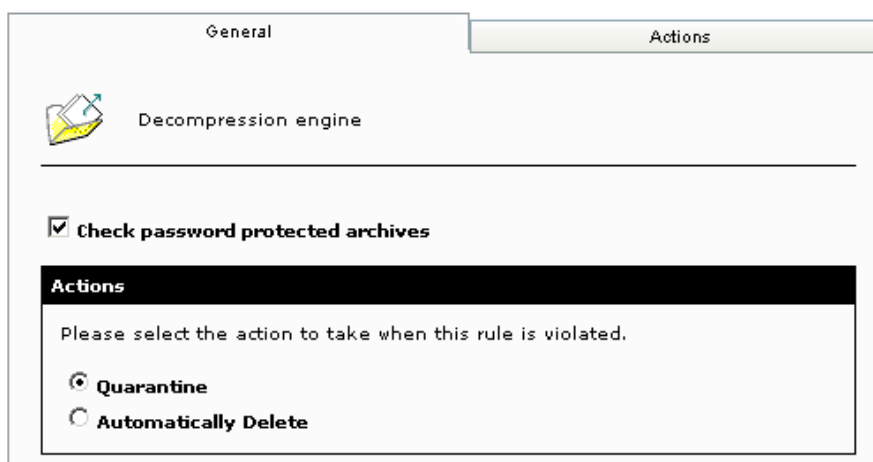
The following is a list of archive filters included in the decompression engine:

- Check password protected archives
- Check corrupted archives
- Check for recursive archives
- Check size of uncompressed files in archives
- Check for amount of files in archives
- Scan within archives

You can configure each of the above listed filters separately. This means that you can specify what each decompression filter should do with emails containing particular archives.

Configuring the decompression engine filters

Check password protected archives



Screenshot 69 - Configuring password protected archives options

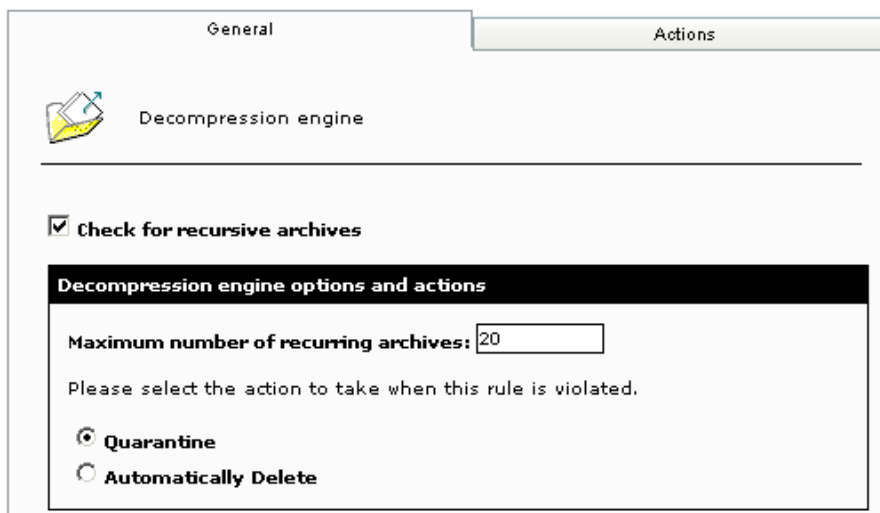
This filter allows you to quarantine or delete emails that contain password-protected archives. To configure this filter:

1. Click the **GFI MailSecurity ► Decompression** node.
2. From the list of available filters (in the right window), click on **Check password protected archives**.
3. Select the **Check password protected archives** check box to enable this filter.
4. Specify what to do with emails containing password-protected archives by selecting one of the following options:
 - **Quarantine** – Select this option to quarantine the emails that contain a password-protected archive. The administrator can later review these quarantined emails and approve or delete them accordingly.
 - **Automatically Delete** – Select this option to delete emails containing password-protected archives.
5. Click the **Actions** tab to configure any actions to be performed whenever an email containing a password-protected archive is detected and blocked. For more information on how to configure actions refer to the 'Configuring decompression filter actions' section in this chapter.
6. Click **Apply**.

Check corrupted archives

This filter allows you to quarantine or delete emails that contain corrupted archives. The configuration options of this filter are identical to those of the 'Check password protected archives'. For more information on how to configure these options, refer to the 'Check password protected archives' section above.

Check for recursive archives



The screenshot shows the 'General' tab of the 'Decompression engine' configuration window. The 'Check for recursive archives' checkbox is checked. Below this, a section titled 'Decompression engine options and actions' contains a text box for 'Maximum number of recurring archives' set to 20. Below the text box, it says 'Please select the action to take when this rule is violated.' There are two radio button options: 'Quarantine' (selected) and 'Automatically Delete'.

Screenshot 70 - Configuring recursive archives options

This filter allows you to quarantine or delete emails that contain recursive archives. Recursive archives, also known as nested archives, are archives that contain other/multiple levels of sub-archives (i.e. archives within archives). A high number of archive levels can indicate a malicious archive: Recursive archives can be used in a DoS (Denial of Service) attack, since most content scanning and anti-virus packages crash while attempting to scan nested archive levels.

To configure this filter:


1. Click the **GFI MailSecurity ► Decompression** node.
 2. From the list of available filters (in the right window), click on **Check for recursive archives**.
 3. Select the **Check for recursive archives** check box to enable this filter and specify the maximum number of nested archives permitted.
- IMPORTANT:** If you disable the **Check for recursive archives** rule, GFI MailSecurity will not scan or quarantine recursive archives, thus bypassing the anti-virus checking.
4. Decide on what to do with emails containing nested archives that exceed the specified limit by selecting one of the following options:

- **Quarantine** – Select this option to quarantine the emails that contain recursive archives. The administrator can later review these quarantined emails and approve or delete them accordingly.
- **Automatically Delete** – Select this option to delete emails containing recursive archives that exceed the specified nesting limit.


5. Click the **Actions** tab to configure any actions to be performed whenever an email containing a recursive archive is detected and blocked. For more information on how to configure actions refer to the 'Configuring decompression filter actions' section in this chapter.

6. Click **Apply**.

Check size of uncompressed files in archives



General Actions

 Decompression engine

☒ Check size of uncompressed files in archives

Decompression engine options and actions

Maximum size of uncompressed files in archive in Mb:

Please select the action to take when this rule is violated.

☒ Quarantine

☐ Automatically Delete

Screenshot 71 - Configuring checks for the size of uncompressed files in archives

This filter allows you to block or delete emails with archives that exceed the specified physical size when uncompressed. Hackers sometimes use this method in a DoS (Denial of Service) attack: By sending an archive that can be uncompressed to a very large file, they can often crash content security or anti-virus software.

To configure this filter:

1. Click the **GFI MailSecurity ► Decompression** node.
2. From the list of available filters (in the right window), click on **Check size of uncompressed files in archives**.
3. Select the **Check size of uncompressed files in archives** check box to enable this feature and specify the maximum size (in MB) allowed for uncompressed files, received within an archive.

IMPORTANT: If you disable the **Check size of uncompressed files in archives** rule, GFI MailSecurity will not scan or quarantine archive attachments, thus bypassing the anti-virus checking.

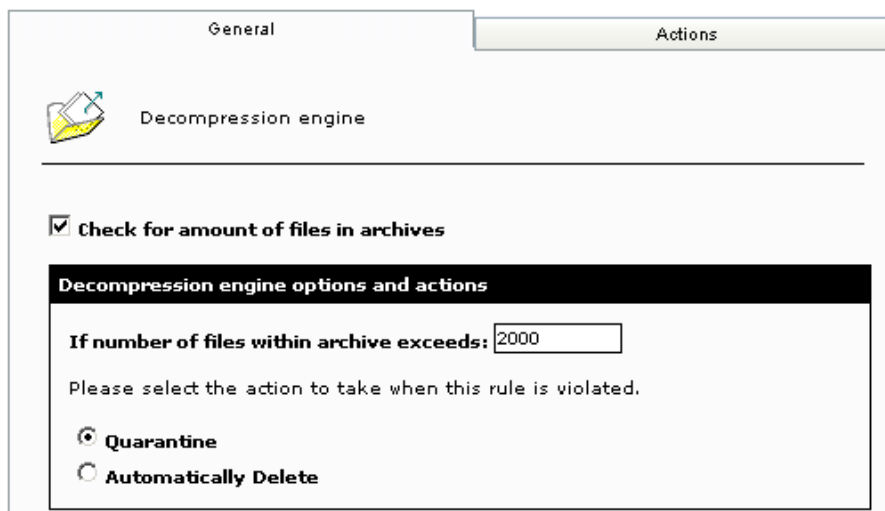
4. Decide on what to do with emails containing archived files that exceed the specified size when un-compressed.

- **Quarantine** – Select this option to quarantine the emails that contain these archives. The administrator can later review these quarantined emails and approve or delete them accordingly.
- **Automatically Delete** – Select this option to delete emails containing archived files that when un-compressed, exceed the specified size limit.

5. Click the **Actions** tab to configure any actions to be performed whenever this filter detects and blocks emails containing an archive. For more information on how to configure actions refer to the 'Configuring decompression filter actions' section in this chapter.

6. Click **Apply**.

Check for amount of files in archives



The screenshot shows the 'General' tab of the 'Decompression engine' configuration window. A checkbox labeled 'Check for amount of files in archives' is checked. Below this, a section titled 'Decompression engine options and actions' contains a text box for 'If number of files within archive exceeds:' with the value '2000'. Below this, there are two radio button options: 'Quarantine' (selected) and 'Automatically Delete'.

Screenshot 72 - Configuring the amount of files in archive check

This filter allows you to quarantine or delete emails that contain an excessive amount of compressed files within an attached archive. You can specify the number of files allowed in archive attachments from the configuration options included in this filter.

To configure this filter:

1. Click the **GFI MailSecurity ► Decompression** node.
 2. From the list of filters (in the right window), click on **Check for amount of files in archives**.
 3. Select the **Check for amount of files in archives** check box to enable this filter and specify the maximum amount of files allowed in an archive.
- IMPORTANT:** If you disable the **Check for amount of files in archives** rule, GFI MailSecurity will not scan or quarantine archive attachments, thus bypassing the anti-virus checking.
4. Decide on what to do with emails containing archives that exceed the specified limit of contained files by selecting one of the following options:
 - **Quarantine** – Select this option to quarantine the emails that contain these archives. The administrator can later review these quarantined emails and approve or delete them accordingly.
 - **Automatically Delete** – Select this option to delete emails containing archived files that when uncompressed contain more files than the limit specified.
 5. Click the **Actions** tab to configure any actions to be performed whenever this filter detects and blocks emails containing an archive. For more information on how to configure actions refer to the 'Configuring decompression filter actions' section in this chapter.
 6. Click **Apply**.

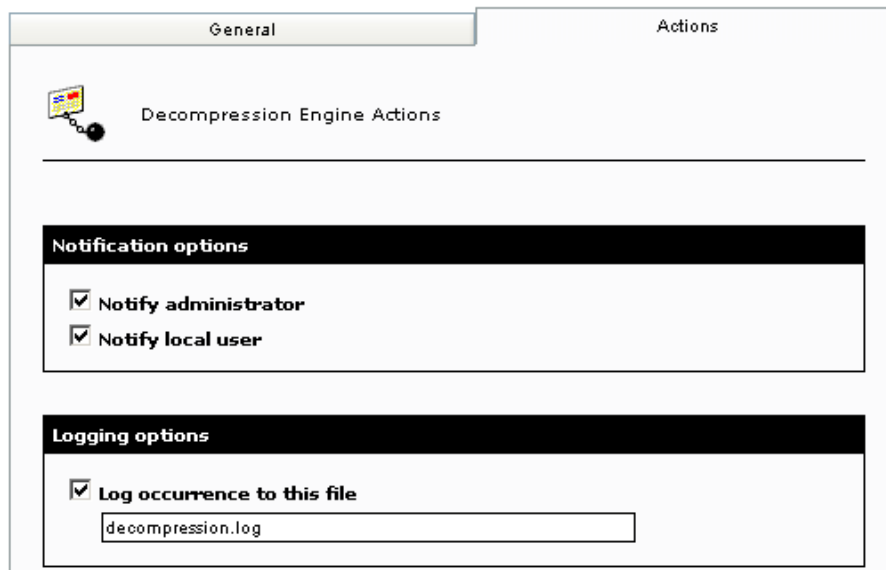
Scan within archives

Through the **Scan within archives** option, you can disable Attachment Checking and Content Checking of files in archives.

Configure this option as follows:

1. Click the **GFI MailSecurity ► Decompression** node.
2. From the list of filters (in the right window), click on **Scan within archives**.
3. Select the **Scan within archives** check box to scan any archive attachments present in an email using the decompression and attachment scanning rules.

Configuring decompression filter actions



General Actions

Decompression Engine Actions

Notification options

- ☒ Notify administrator
- ☒ Notify local user

Logging options

- ☒ Log occurrence to this file
decompression.log

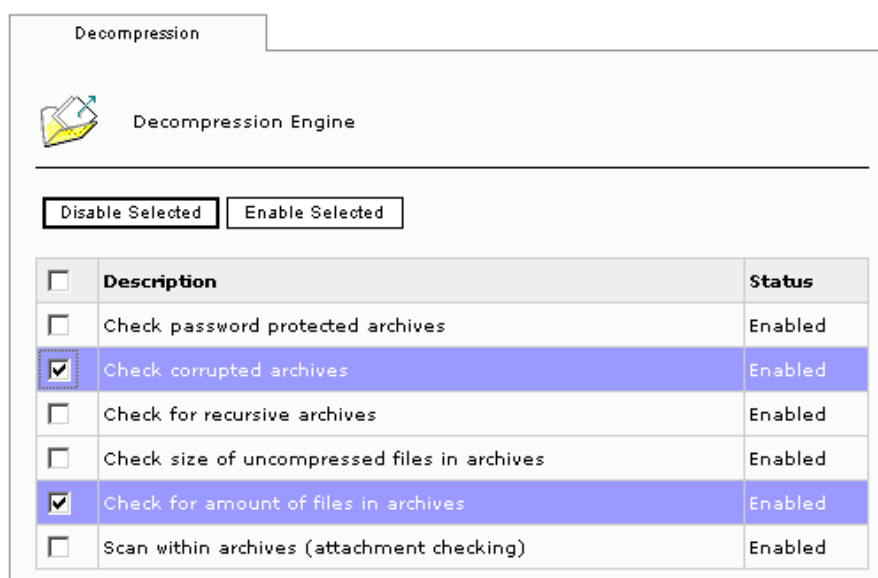
Screenshot 73 - Decompression filter actions

To configure the actions to be performed whenever a particular filter blocks emails containing archives:

1. Click the **GFI MailSecurity ► Decompression** node and from the right window select the required filter.
2. Click the **Actions** tab and select any of the following actions:
 - **Notify local user** – Select this option if you want to notify the email local users when the email contains an archive file that infringes a decompression engine rule.

NOTE: If a threat is detected in an outbound email, the recipients will receive the original email with the malicious parts removed. A security notice is attached to the email to inform the recipients what email parts were removed and for what reason. This behavior is always enabled and is not affected by this setting.
 - **Notify administrator** – Select this option to send email notifications to the administrator whenever an email containing an archive is quarantined.
 - **Log occurrence to this file** – Select this option to log the event whenever the selected decompression filter blocks an email. In the box below, specify either a file name only or the full path to the log file.
3. Click **Apply**.

Enable/disable decompression filters



Screenshot 74 - Decompression tool filters list

To enable or disable any of the available decompression filters:

1. Click the **GFI MailSecurity ► Decompression** node.
2. In the right window, select the check box of the filter(s) that you want to enable or disable.
3. Click **Enable selected** or **Disable selected** accordingly.

NOTE: You can select all check boxes in one go by selecting the check box next to the **Description** column heading at the top-left of the list.

The Trojan & Executable Scanner

Introduction to the Trojan & Executable Scanner

GFI MailSecurity includes an advanced Trojan and Executable Scanner, which is able to analyze and determine the function of an executable file. This scanner can subsequently quarantine any executables that perform suspicious activities (such as a Trojan).

What is a Trojan horse?

The Trojan horse got its name from the old mythical story about how the Greeks gave their enemy a huge wooden horse as a gift during the war. The enemy accepted this gift and brought it into their fortress. During the night, Greek soldiers crept out of the horse and attacked the city.

In computers a Trojan horse is a way of penetrating a victim's computer undetected, allowing the attacker unrestricted access to the data stored on that computer. Subsequently the attacker can manipulate the data and can cause great damage to the victim, just like the citizens of Troy.

A Trojan can be a hidden program that runs on your computer without your knowledge. Furthermore, hackers sometimes hide Trojans into legitimate programs that you normally use.

Difference between Trojans and viruses

The difference between Trojans and viruses is that Trojans are often 'one-off' ('tailor made') executables, targeted to obtain information from a specific target (user/system). In general, a hacker deploys a Trojan to create a backdoor on a system, thus gaining unrestricted access to the system. Signature based anti-virus software, are unable to detect one-off Trojans. Indeed any application that only uses signatures to detect malicious software will not be effective in detecting such threats. These include specialized anti-Trojan software. The main reason is that signature based software can only detect known viruses and Trojans. That is why such applications need frequent updates.

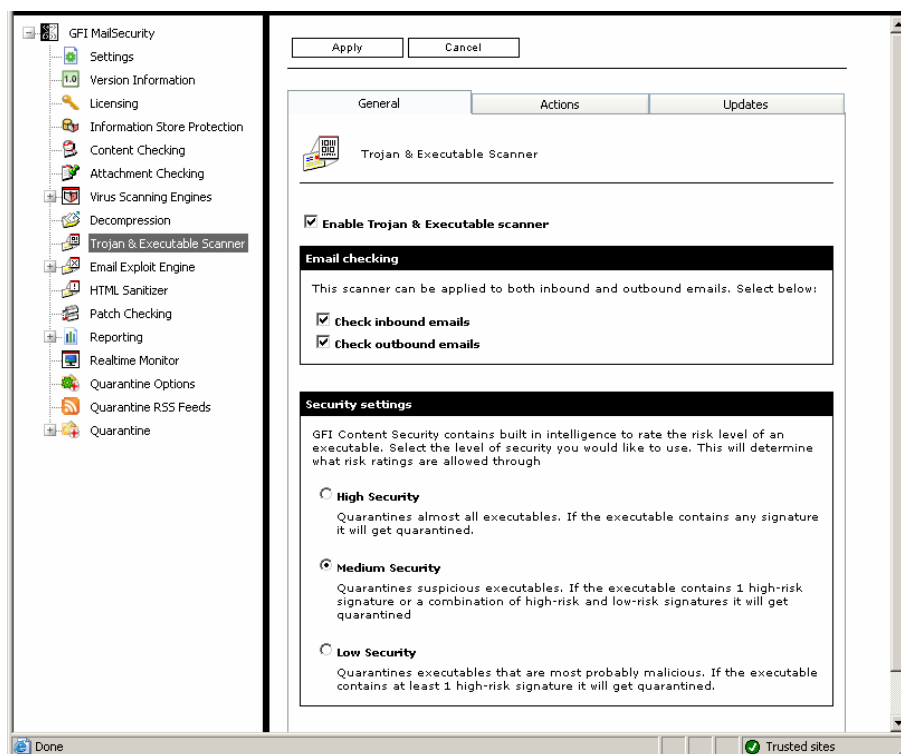
How does the Trojan & Executable Scanner work?

GFI MailSecurity is able to rate the risk-level of an executable file by decompiling the executable, and detecting in real time what the executable might do. Subsequently, it compares capabilities of the executable to a database of malicious actions and then rates the risk level of this executable file. With the Trojan & Executable scanner, you can detect and block potentially dangerous, unknown or one-off Trojans before they penetrate your network.

Configuring the Trojan & Executable Scanner

From the **Trojan & Executable Scanner** node, you can define the level of security that you require and the actions you want GFI MailSecurity to take on emails containing malicious executable files.

Configuring the security level



Screenshot 75 - Trojan and Executable Scanner: General Tab

To configure the Trojan & Executable Scanner:

1. Click the **GFI MailSecurity ► Trojan & Executable Scanner** node.
2. From the configuration options (in the right window), select the **Enable Trojan & Executable Scanner** check box to activate this filter.
3. Specify the emails you want to check for Trojans and other malicious executables by selecting any of the following options:
 - **Check inbound emails** – Select this option to scan inbound emails for Trojans and malicious executable files.
 - **Check outbound emails** - Select this option to scan outbound emails for Trojans and malicious executable files.
4. Choose the required level of security by selecting one of the following options:
 - **High Security** - Select this option to quarantine almost all executables. If the executable file contains any known malicious signature it will get immediately quarantined.
 - **Medium Security** - Select this option to quarantines only suspicious executables. If the executable contains one high-risk signature or a combination of high-risk and low-risk signatures it will be quarantined.

- **Low Security** - Select this option to quarantine all malicious executables. If the executable contains at least one high-risk signature, it will be immediately quarantined.

Configuring actions

Screenshot 76 - Trojan and Executables Scanner: Actions Tab

5. Click the **Actions** tab to configure the actions you want GFI MailSecurity to take on emails containing a malicious executable. Select any of the following options:

- **Notify local user** – Select this option if you want to notify the email local users when this filter detects a malicious executable.
NOTE: If a threat is detected in an outbound email, the recipients will receive the original email with the malicious parts removed. A security notice is attached to the email to inform the recipients what email parts were removed and for what reason. This behavior is always enabled and is not affected by this setting.
- **Notify administrator** – Select this option to send email notifications to the administrator whenever an email containing malicious executable is quarantined.
- **Log occurrence to this file** – Select this option to log the event whenever the Trojan & Executable Scanner detects an infected email. In the edit box below, specify either the file name only or the full path to the log file.

6. Click **Apply**.

Trojan & Executable Scanner updates

You can configure GFI MailSecurity to download Trojan & Executable Scanner updates automatically or to notify the administrator whenever new updates are available. To configure automatic updates:

1. Click the **GFI MailSecurity ► Trojan & Executable Scanner** node.
2. Click the **Updates** tab in the Trojan & Executable Scanner page (in the right window).

3. Select the **Automatically check for updates** check box to enable the auto-update feature.
 4. From the **Downloading options** list, select one of the following download options:
 - **Only check for updates** – Select this option if you want GFI MailSecurity to just check and notify the administrator whenever updates are available for the Trojan & Executable Scanner.
- NOTE:** This option will NOT download the available updates.
- **Check for updates and download** – Select this option if you want GFI MailSecurity to check and automatically download any updates available for the Trojan & Executable Scanner.
5. Specify how often you want GFI MailSecurity to check/download updates for the Trojan & Executable Scanner, by typing an interval in hours.
 6. Click **Apply**.

General Actions Updates

Trojan & Executable Scanner Updates

Automatic update options

Configure the automatic update options.

☒ **Automatically check for updates**

Downloading option:

Check for updates and download

Download/check after the specified number of hours:

1

Last update:

Update options

☒ **Enable email notifications upon successful updates (Notifications will always be sent for unsuccessful updates).**

Click the button below to force the updater service to download the most recent updates.

Download updates

Screenshot 77 - Trojan and Executable Scanner: Updates tab

Triggering the Trojan & Executable Scanner update manually

To check/download updates for the Trojan & Executable Scanner immediately, click **Download updates**.

The Email Exploit Engine

Introduction to e-mail exploits

What is an exploit?

An exploit uses known vulnerabilities in applications or operating systems to compromise the security of a system, for example, execute a program or command, or install a backdoor. It "exploits" a feature of a program or the operating system for its own use.

What is an e-mail exploit?

An email exploit is an exploit launched via email. An email exploit is essentially an exploit that can be embedded in an email, and executed on the recipient's machine either once the user opens or receives the email. This allows the hacker to bypass firewalls and anti-virus products.

Difference between Anti-Virus software & Email Exploit Detection software

Anti-virus software is designed to detect malicious code. It does not necessarily analyze the method used to execute the code.

The Email Exploit Detection Engine analyses emails for exploits - i.e., it scans for methods to execute a program or command on the user's system. The Email Exploit Engine does not check whether the program is malicious or not. Rather, it assumes a security risk if an email is using an exploit in order to run a program or command - whether or not the actual program or command is malicious.

In this manner, the Email Exploit Engine works like an intrusion detection system (IDS) for email. The Email Exploit Engine might cause more false-positives, but it is more secure than a normal anti-virus package, simply because it uses a different way of checking for e-mail threats.

Furthermore, the Email Exploit Engine is optimized for finding exploits in email, and can therefore be more effective at this job than a general-purpose anti-virus engine.

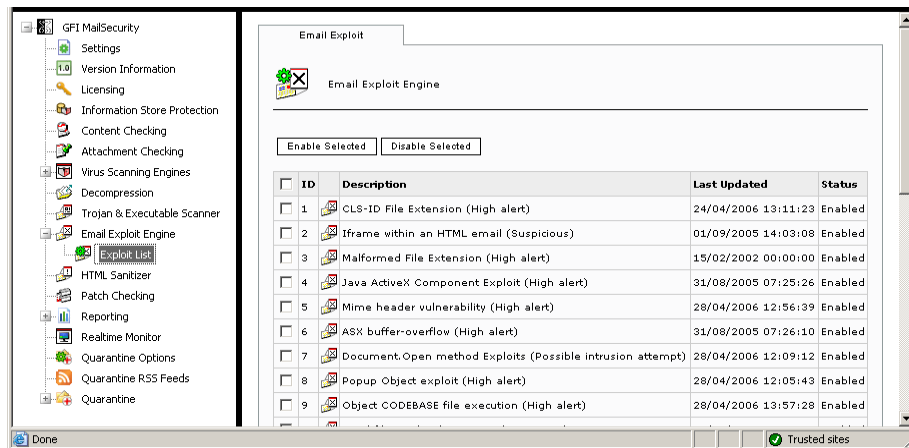
Configuring the Email Exploit Engine

Enable/Disable email exploits

To enable/disable emails exploits:

1. Click the **GFI MailSecurity ► Email Exploit Engine ► Exploit List** node.

2. From the Email Exploit Engine page (in the right window), select the check box of the exploit(s) that you want to enable or disable.
3. Click **Enable Selected** or **Disable Selected** accordingly. The status change is displayed immediately in the exploits **Status** column.

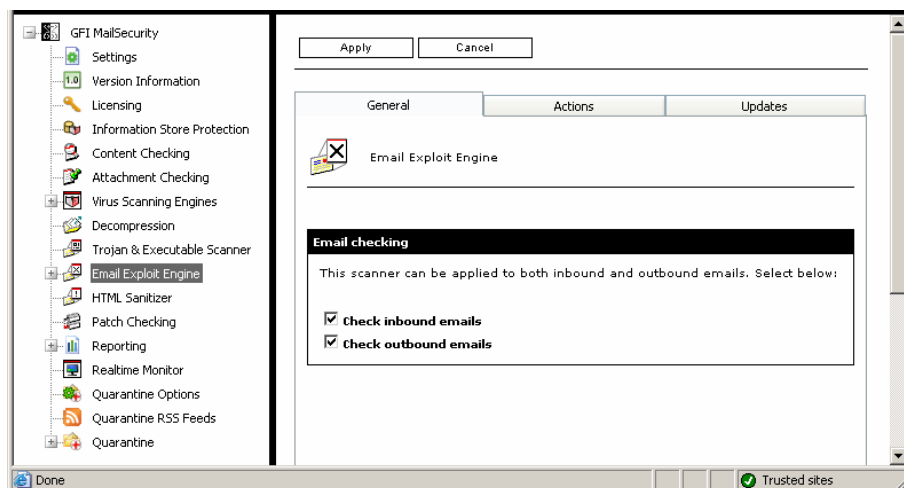


Screenshot 78 - Email Exploit list

Configuring the Email Exploit Engine properties

To configure the **Email Exploit Engine** properties:

1. Click the **GFI MailSecurity ► Email Exploit Engine** node.
2. From the **General** tab, select whether you want to check inbound and/or outbound emails for email exploits, by selecting the **Check inbound emails** check box and **Check outbound emails** check box accordingly.



Screenshot 79 - Email Exploit Engine: General Tab

3. Click on the **Actions** tab, to set what actions you want GFI MailSecurity to take on emails containing email exploits.
4. You can choose either one of the following options:
 - **Quarantine email:** Select this option to quarantine the email containing the email exploit for review by an administrator. For more information, refer to the 'Quarantining' chapter in this manual.

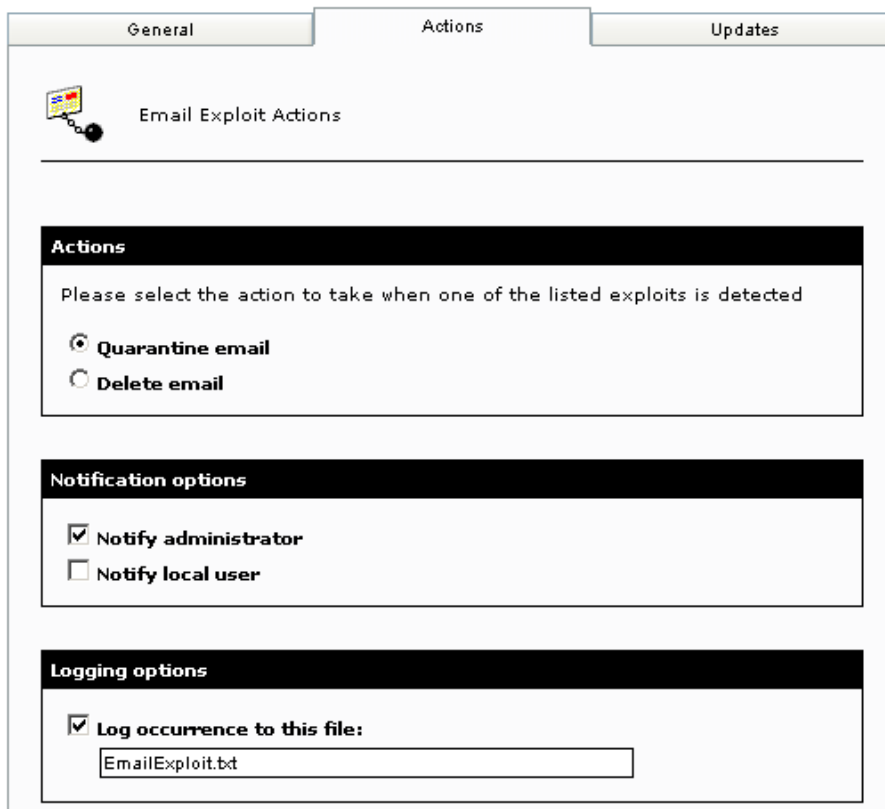
- **Delete email:** Select this option to delete the email containing the email exploit completely.

5. When an email exploit is detected, you can also choose to inform the administrator and/or user by sending email notifications. You can configure the required notifications by selecting any of the following options:

- **Notify local user:** Select this option if you want to notify the email local users when this filter detects an email exploit.

NOTE: If a threat is detected in an outbound email, the recipients will receive the original email with the malicious parts removed. A security notice is attached to the email to inform the recipients what email parts were removed and for what reason. This behavior is always enabled and is not affected by this setting.

- **Notify administrator:** Select this option if you want to send email notifications to the administrator whenever an email containing email exploits is detected. The administrator's email address is specified during the installation of GFI MailSecurity but can still be changed from the GFI MailSecurity configuration (**GFI MailSecurity** ► **Settings** node ► **General** tab). For more information refer to the 'Define the administrator's email address' section in the General Settings chapter.



The screenshot shows the 'Email Exploit Actions' configuration window with three tabs: 'General', 'Actions', and 'Updates'. The 'Actions' tab is selected. The window contains three main sections: 'Actions', 'Notification options', and 'Logging options'. In the 'Actions' section, 'Quarantine email' is selected with a radio button, and 'Delete email' is unselected. In the 'Notification options' section, 'Notify administrator' is checked with a checkbox, and 'Notify local user' is unchecked. In the 'Logging options' section, 'Log occurrence to this file:' is checked, and the text 'EmailExploit.txt' is entered in the adjacent text box.

Screenshot 80 - Email Exploit Engine: Actions Tab

6. Select the **Log occurrence to this file** check box if you want to log all email exploits detected to a log file. In the box below, specify either a file name only or the full path to the log file.

7. Click **Apply**.

Email Exploit Engine updates

You can configure GFI MailSecurity to download Email Exploit Engine updates automatically or to notify the administrator whenever new updates are available. To configure automatic updates:

1. Click the **GFI MailSecurity ► Email Exploit Engine** node.
2. Click the **Updates** tab.
3. Select the **Automatically check for updates** check box to enable the auto-update feature.
4. From the **Downloading option** list, select one of the following download options:

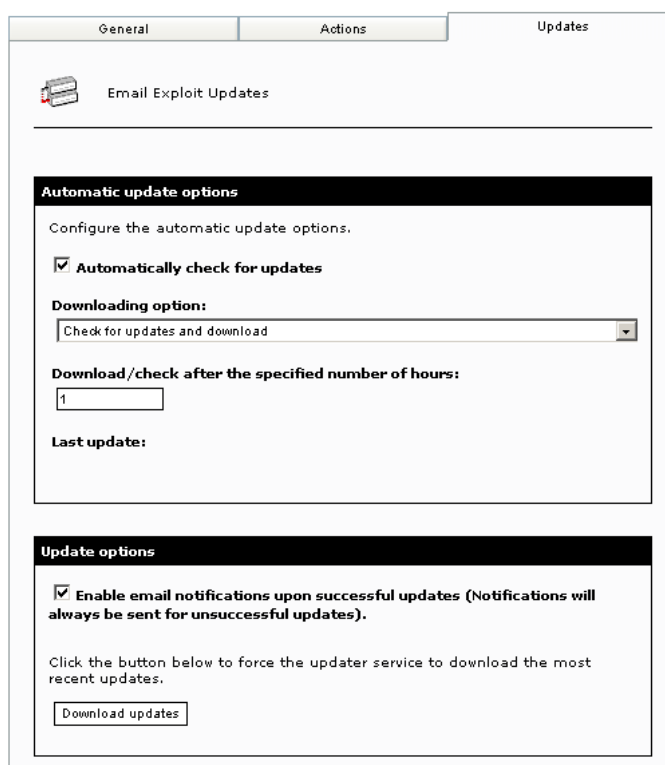
- **Only check for updates** – Select this option if you want GFI MailSecurity to just check and notify the administrator whenever updates are available for the Email Exploit Engine.

NOTE: This option will NOT download the available updates.

- **Check for updates and download** – Select this option if you want GFI MailSecurity to check and automatically download any updates available for the Email Exploit Engine.

5. Specify how often you want GFI MailSecurity to check/download updates for the Email Exploit Engine, by typing an interval in hours.

6. Click **Apply**.



The screenshot shows the 'Updates' tab of the 'Email Exploit Updates' configuration window. It has three tabs: 'General', 'Actions', and 'Updates'. The 'Updates' tab is active. Below the title bar, there is a section titled 'Automatic update options' with a sub-header 'Configure the automatic update options.' It contains a checked checkbox for 'Automatically check for updates', a dropdown menu for 'Downloading option:' set to 'Check for updates and download', a text input field for 'Download/check after the specified number of hours:' with the value '1', and a 'Last update:' label. Below this is another section titled 'Update options' with a checked checkbox for 'Enable email notifications upon successful updates (Notifications will always be sent for unsuccessful updates).' and a 'Download updates' button.

Screenshot 81 - Email Exploit Engine: Updates Tab

Triggering the Email Exploit Engine update manually

To check/download updates for the Email Exploit Engine immediately, click **Download updates**.

The HTML Sanitizer

Introduction to the HTML Sanitizer

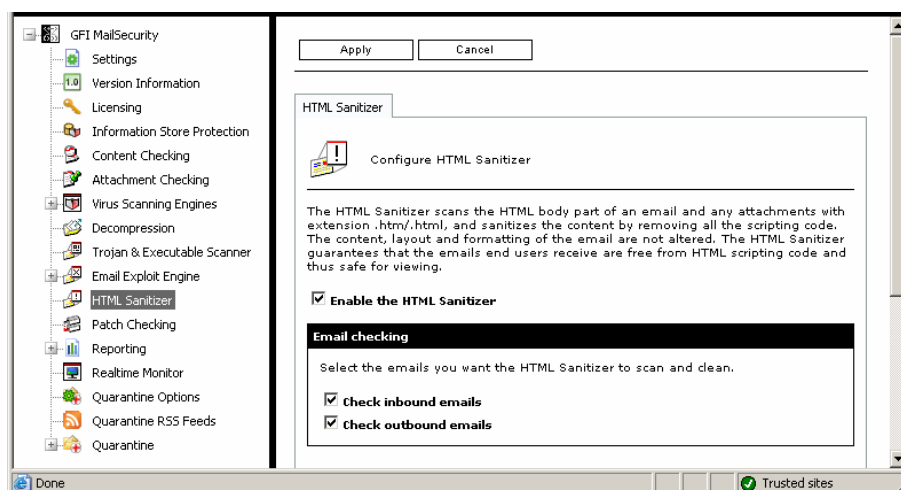
The HTML Sanitizer scans and cleans from scripting code the email body parts that have the MIME type set to “text/html” and all the attachments that have an extension of “.htm” or “.html”. The HTML is cleaned from all the scripts, rendering it harmless. The HTML sanitization process is an automated process, which does not require administrator intervention.

Why remove HTML scripts?

The introduction of HTML mail has allowed senders to include scripts in email that can be triggered automatically upon opening mail. HTML scripts are used in a number of headline hitting viruses, such as the KAK worm. Moreover, HTML scripts are often utilized in one-off attacks directed towards particular users and particular companies. Consequently, it is best if all scripts are removed from within HTML emails.

The HTML Sanitizer included in GFI MailSecurity provides automated protection against HTML scripting threats.

Configuring the HTML Sanitizer



Screenshot 82 - HTML Sanitizer configuration page

Configure the HTML Sanitizer as follows:

1. Click the **GFI MailSecurity ► HTML Sanitizer** node.
2. From the **HTML Sanitizer** configuration page, select the **Enable the HTML Sanitizer** check box to enable the HTML Sanitizer.

3. Select the emails you want to check for HTML scripts and clean by selecting any of the following options:

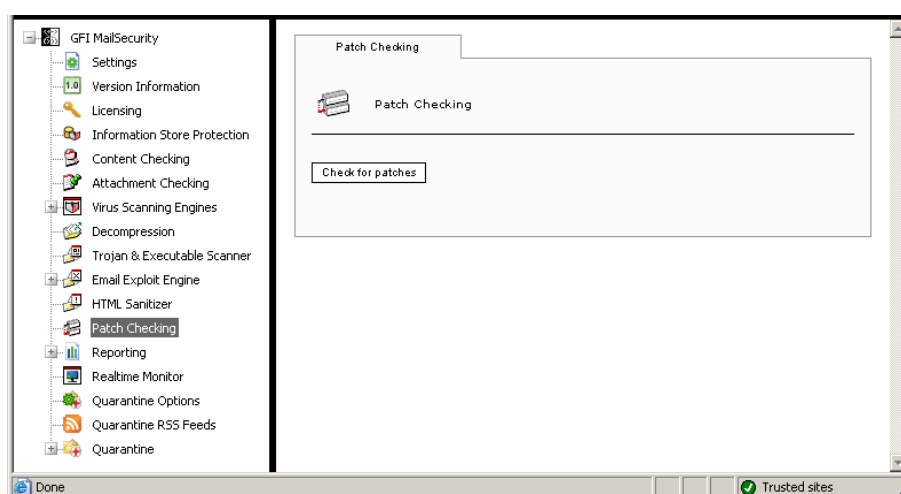
- **Check inbound emails** – Select this option to scan and clean HTML scripts from all inbound emails.
- **Check outbound emails** – Select this option to scan and clean HTML scripts from all outbound emails.

4. Click **Apply**.

Patch Checking

Introduction to Patch Checking

The Patch Checking feature verifies if there are any software patches available for your version of GFI MailSecurity by directly connecting/querying the GFI Update Servers.



Screenshot 83 - List of available patches

If software updates are present on the GFI Servers, this feature lists them out for you to download. In addition, the list of available updates includes links to information about each patch as well as to the relative GFI Knowledge Base articles if available.

NOTE 1: In order to keep GFI MailSecurity running efficiently, we recommend that you periodically check for software updates. These updates would help to ensure better performance and enhance the functionality of GFI MailSecurity.

NOTE 2: For more information on how to specify the GFI Update Server, to which GFI MailSecurity will connect when checking for software updates, refer to the 'Selecting an update server' section in the 'General Settings' chapter.

Downloading and installing software patches

To check for GFI MailSecurity software updates:

1. Click the **GFI MailSecurity ► Patch Checking** node, and click **Check for patches** in the right pane window, to connect to the GFI Update Server and check for available updates.
2. If software patches exist for your version of GFI MailSecurity, these are listed in the right window. Otherwise, you will be informed that no software patches are available. From the list of available software

updates (in the right window), click the **Download** link included in the last column of each patch. This will start the download process. Repeat the same procedure for all the listed updates.

3. After all downloads are complete, you can start installing the software updates. Since the software patches vary in file format (i.e. could be DLL files, EXE files, etc.), you must read the relative patch information for the installation instructions. To access the installation instructions and other information relevant to a patch, click the **Information** link provided in the list of available updates (in the right window of GFI MailSecurity).

NOTE 1: It is important that you follow the exact patch instructions provided in the information link. An incorrect patch installation might cause a product malfunction or degrade its performance.

NOTE 2: If available, GFI MailSecurity also includes links to Knowledge Base articles related to the listed patches. This is denoted by the **KB Article** caption in the KB link column of the patch. To access the Knowledge Base information, click the **KB Article** caption/link.

NOTE 3: GFI MailSecurity sends an email notification to the administrator whenever new software patches are discovered.

Quarantine

Introduction to the Quarantine Store

As outlined earlier in the manual, you can configure GFI MailSecurity to quarantine the emails that fail any of the content policy or content security checks. You can then review the quarantined emails and either approve or delete them.

You can approve/delete quarantined emails either directly from the Quarantine Store or through a Quarantine Action Form.

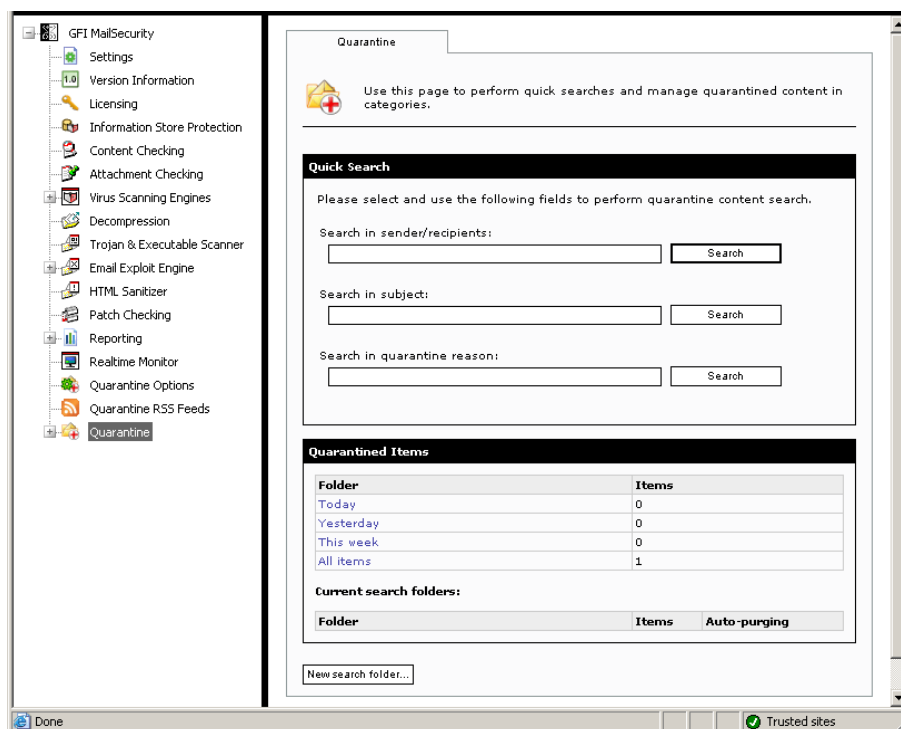
- Approve/Delete directly from the Quarantine Store (recommended). For more information on how to review emails in the Quarantine Store, refer to the 'Approving emails from the Quarantine Store' section, further on in this chapter.
- Approve/Delete from a Quarantine Action Form. GFI MailSecurity sends the Quarantine Action Form through email to the administrator (on the administrator's email address) or to a specific email address, belonging to an authorized person who can review quarantined emails. For more information, refer to the 'Enable email approval via HTML approval forms' section further on in this chapter.

The Quarantine Store

To access the GFI MailSecurity Quarantine Store, click the **GFI MailSecurity ► Quarantine** node. From the **Quarantine** node, the administrator/authorized user can search for quarantined emails as well as approve or delete emails.

When you click the **Quarantine** node, GFI MailSecurity displays the following:

- Quick Search – You can search for quarantined emails by sender, recipient, subject or quarantine reason.
- Quarantined Items – You can see how many emails are currently stored in the Quarantine Store and the amounts that match each quarantine search folder, be it default or custom. To view the quarantined emails contained in a search folder, click on the quarantine search folder name. Refer to the 'Grouping quarantined emails in Search Folders' section further on in this chapter, for information on how to create and use search folders. To access this information from the navigation panel, expand the **Quarantine** node and click on a sub-node.



Screenshot 84 - Quarantine Store status page

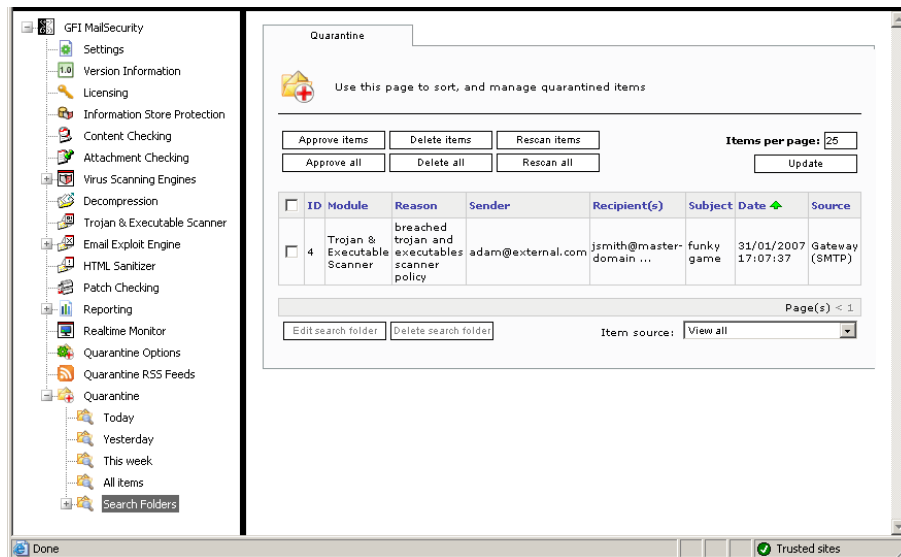
Searching for emails in the Quarantine Store

Screenshot 85 - Quarantine Store: Quick Search

To search for emails in the GFI MailSecurity Quarantine Store, follow these steps:

1. Click on either the **GFI MailSecurity ► Quarantine** node or the **GFI MailSecurity ► Quarantine ► Search Folders** node.
2. From the **Quick Search** area, use one of these methods to perform the search:
 - **Search in sender/recipients** – Specify an email address and click **Search** to find quarantined emails sent from or received by that email address.
 - **Search in subject** – Specify a keyword or phrase and click **Search** to find quarantined emails that contain that specific word/string in the subject.

- **Search in quarantine reason** – Specify a keyword or phrase and click **Search** to find quarantined emails that contain that specific word/string in the quarantine reason.



Screenshot 86 – Quick search results

Search Folders

What is a search folder?

A Search Folder is a special type of folder that has a search query associated to it. The contents of the search folder are the quarantined emails that match the search query. The content of a search folder is thus dynamic and changes automatically as emails that match the search folder criteria are quarantined or deleted.

Why are search folders useful?

The main benefit of search folders is that they help you organize your quarantined emails. In this way, it is easier for the administrator to identify and then approve or delete blocked emails.

Each search folder can have different search criteria, thus you can virtually split the Quarantine Store into subdivisions containing emails with specific characteristics in each group. For example, you can create a search folder that collects only emails that were quarantined by the Virus Scanning Engines. A good idea is to create a search folder for each GFI MailSecurity module, so that instead of viewing one huge list of quarantined emails, you split them up into logical groups.

Grouping quarantined emails in Search Folders

To create a new search folder, follow these steps:

1. Click on either the **GFI MailSecurity ► Quarantine** node or the **GFI MailSecurity ► Quarantine ► Search Folders** node.
2. From the right panel, click **New search folder**.

3. In the **Search folder name** box, type a name for the new search folder, for example, "Emails blocked by Attachment Rules".

4. If you installed GFI MailSecurity on the Microsoft Exchange Server machine, you can limit the emails in this search folder to those blocked from a particular source. From the list under the **Item source** area, you can select one of the following:

- **Information store (VSAPI)** – Only quarantined items forming part of the Information Store will be displayed.
- **Information store (Transport)** – This option is only available when GFI MailSecurity is installed on a Microsoft Exchange Server 2007 machine with the Hub Transport Server Role installed. Only quarantined items forming part of the Information Store that were scanned through the Hub Transport Agent will be displayed.
- **Gateway (SMTP)** – Only inbound or outbound quarantined emails, SMTP traffic, will be displayed.
- **Any** – All quarantined items will be displayed irrespective of the source.

5. You can now configure auto-purge settings for this search folder. If you configure auto purging on a search folder, GFI MailSecurity will delete any emails in that search folder that are older than the number of days you specify.

To enable auto-purging, select the **Enable Auto-purging** check box and specify a value in the **days(s)** box.


NOTE: Configure auto purging with great care since emails purged from the Quarantine Store are not recoverable.

6. Specify the search criteria that will determine the contents of this folder. You can select any of the following options:

- **Quarantine reason** – Select this option to include all the emails containing a specific keyword or phrase in the quarantine reason. Type a keyword in the box next to this option.
- **Item subject** – Select this option to include all the emails containing a specific keyword or phrase in the email subject. Type a keyword/phrase in the box next to this option.
- **Sender** – Select this option to include ONLY the emails sent from a particular email address. Type the sender email address in the box next to this option.
- **Recipient** – Select this option to include ONLY the emails sent to a particular email address. Type a recipient email address in the box next to this option.
- **Quarantined by** - Select this option to group emails quarantined by a specific (but not necessarily unique) filter in this search folder. Select a filter from the list next to this option (for example, Attachment Checking).

NOTE: Since GFI MailSecurity can block an email for multiple security threats or content policy infringements, you can choose to include only emails that were blocked by one specific filter. This is possible by selecting the **only** check box next to the filters list.

New Search Folder

 Use this page to create and edit search folders.

Define a new folder

Search folder name:

Item source

Please select item source.

Auto-Purging

With the auto-purge option, you can automate the management of the items stored in this search folder. Items that have been quarantined for at least the number of days you specify will be automatically deleted from the quarantine system.

☒ **Enable Auto-purging**

Automatically purge items older than:

days(s)

Keyword search

Quarantine reason:
☐

Item subject:
☐

Sender:
☐

Recipient:
☐


Search options


Quarantined by:
☒ ☒ **only**

Item direction:
☒

Date filter

☐ **Date:**

Day from:  **Time from: (hh:mm:ss:am/pm)**


Day to:  **Time to: (hh:mm:ss:am/pm)**

Screenshot 87 - New Search Folder properties page

- **Item direction** – Select this option to limit the items included in this search folder to either Inbound or Outbound emails.

NOTE 1: Leave this option unselected if you want to include both Inbound and Outbound emails in this Search Folder.

NOTE 2: This option is only enabled when GFI MailSecurity is not installed on a Microsoft Exchange machine, or if it is, the **Item source** selected was **Gateway**.

- **Date** - Select this option to group emails by date. Specify a date in the relevant box or alternatively click the calendar  button and select the required date from the calendar window.

Specify a Date Range

You can also group emails by Date Range. To do so, click **Date Range**, and then specify a start date in the **Day from** box and an end date in the **Day to** box.

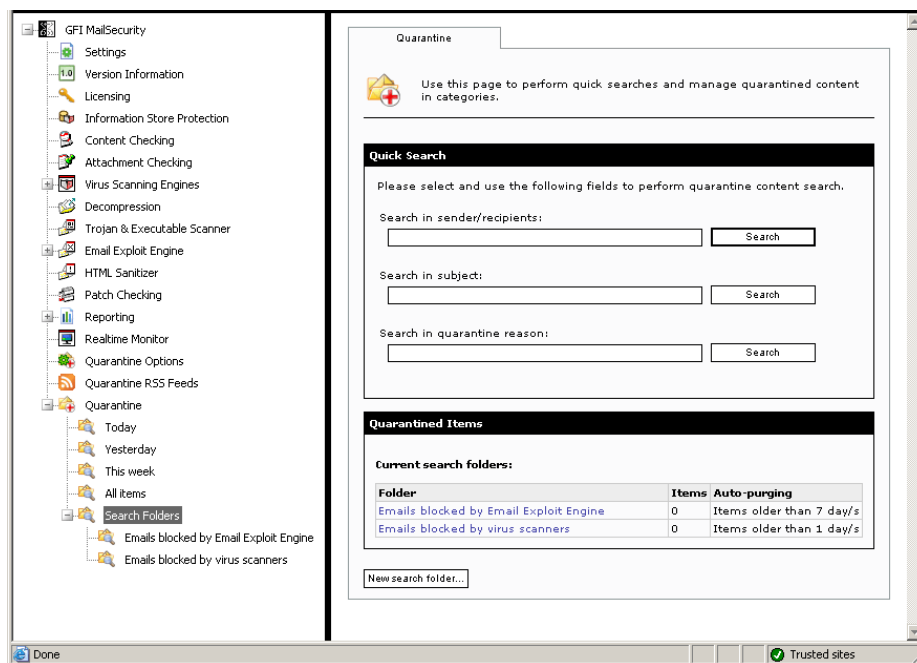
Specify time

In addition to the date, you can also specify the time or time range of the emails you want to include in this folder. To specify the time, select the time check box and input a time value in the relevant box.

Specify time range

To specify a time range for a particular day, click **Date Range** and specify the same date value in both the **Day** boxes. Subsequently specify the required start time in the **Time from** box and the end time in the **Time to** box.

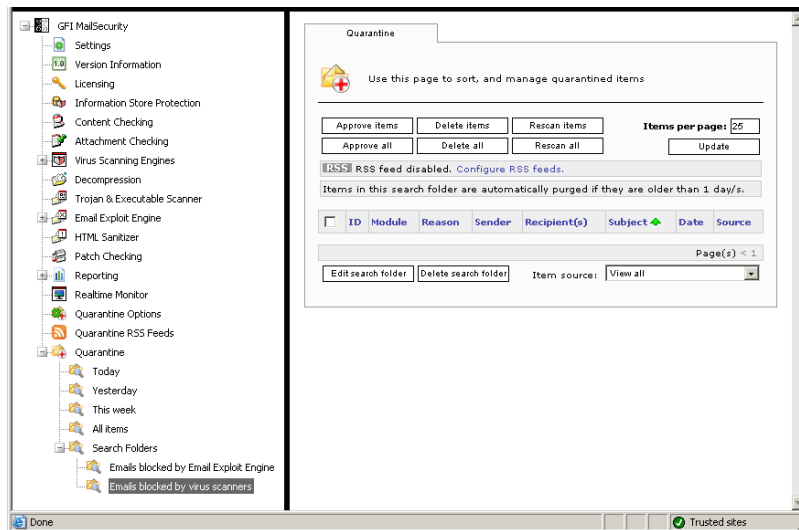
7. Click **Save folder** to create the search folder.



Screenshot 88 - Search Folder Contents Summary

NOTE: Click the **Search Folder** node to view the amount of emails matching each Search Folder.

Changing Search Folder properties



Screenshot 89 - Search Folder options

To modify the properties, search criteria and auto-purge settings of an existing search folder:

1. Expand the **GFI MailSecurity ► Quarantine ► Search Folders** node.
2. Click on the Search Folder you want to modify and from the right pane, click **Edit search folder**.
3. Make the required changes to the search folder properties. For more information on how to configure search folder options, refer to the 'Grouping quarantined emails in Search Folders' section earlier in this chapter.
4. Click **Save folder**.

Deleting Search Folders

To delete an existing search folder:

1. Expand the **GFI MailSecurity ► Quarantine ► Search Folders** node.
2. Click on the Search Folder you want to delete and from the right pane, click **Delete search folder**.

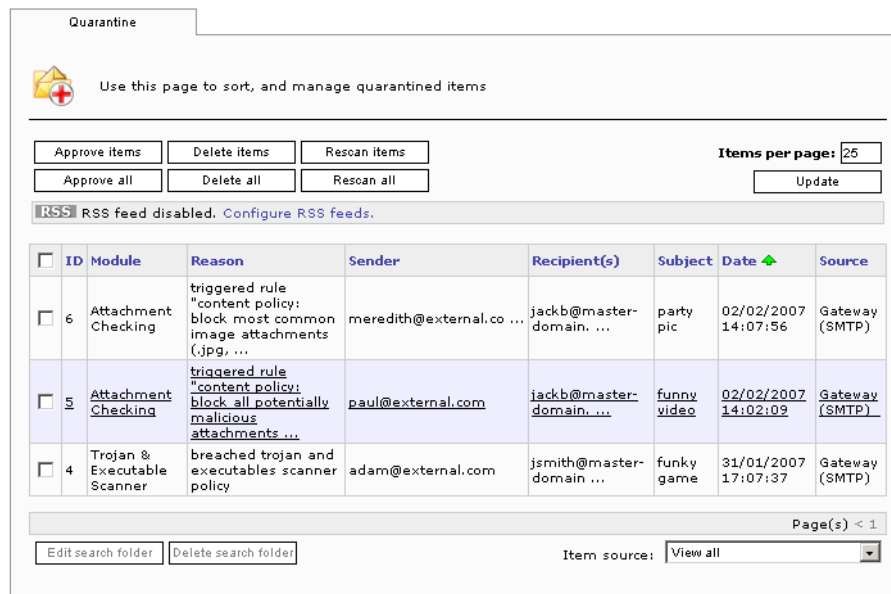
NOTE: - When you delete a search folder, no emails are actually deleted from the quarantine store. This is because a search folder is just a query that retrieves matching emails from the Quarantine Store. In other words, a search folder is just a visual grouping of emails that match certain criteria, but the actual email is not physically stored in the search folder. However, you can still approve or delete emails from within a search folder by using the **Approve items / Delete items** buttons.

Approving emails from the Quarantine Store

You can approve emails from any sub-node underneath the **Quarantine** node including the Search Folders. You can also use Quick Search to look for specific emails that you want to approve. To approve emails:

1. Expand the **GFI MailSecurity ► Quarantine** node and select the sub-node that contains the email(s) you want to approve (for example, select the **Today** node if you want to approve emails that were quarantined today). Alternatively, you can use Quick Search to look for the emails that you want to approve.

NOTE: You can approve an email that was quarantined today from the **Today** node, the **This Week** node, the **All Emails** node as well as from any Search Folder that contains the email. The difference between the mentioned nodes is the amount of emails that are present within.



The screenshot shows the 'Quarantine' page in GFI MailSecurity. It includes a header with a folder icon and the text 'Use this page to sort, and manage quarantined items'. Below this are buttons for 'Approve items', 'Delete items', 'Rescan items', 'Approve all', 'Delete all', 'Rescan all', and an 'Update' button. A message states 'RSS feed disabled. Configure RSS feeds.' Below this is a table of quarantined items with columns: ID, Module, Reason, Sender, Recipient(s), Subject, Date, and Source. The table contains three rows of data. At the bottom, there are buttons for 'Edit search folder' and 'Delete search folder', a 'Page(s) < 1' indicator, and an 'Item source' dropdown menu set to 'View all'.

<input type="checkbox"/>	ID	Module	Reason	Sender	Recipient(s)	Subject	Date	Source
<input type="checkbox"/>	6	Attachment Checking	triggered rule "content policy: block most common image attachments (.jpg, ...)	meredith@external.co ...	jackb@master-domain. ...	party pic	02/02/2007 14:07:56	Gateway (SMTP)
<input type="checkbox"/>	5	Attachment Checking	triggered rule "content policy: block all potentially malicious attachments ..."	paul@external.com	jackb@master-domain. ...	funny video	02/02/2007 14:02:09	Gateway (SMTP)
<input type="checkbox"/>	4	Trojan & Executable Scanner	breached trojan and executables scanner policy	adam@external.com	jsmith@master-domain. ...	funky game	31/01/2007 17:07:37	Gateway (SMTP)

Screenshot 90 - List of Quarantined Emails in selected Search Folder

NOTE: You can sort the quarantined emails by clicking on any of the column headings. If you click the same column heading, the sort order switches between ascending and descending.

2. Select the check box of the email(s) you want to approve and click **Approve items**.

NOTE 1: If you want to approve all the listed emails, you do not need to select all the check boxes individually. Just click **Approve all**.

NOTE 2: To refresh the information, click **Update**.

NOTE 3: If an email matches more than one search folder, the administrator does not need to approve the same email from each search folder. If you approve an email from a search folder, GFI MailSecurity removes it from the Quarantine Store and so it does not list in any of the other search folders.

Deleting emails from the Quarantine Store

To delete emails from the Quarantine Store:

1. Expand the **GFI MailSecurity ► Quarantine** node and select the sub-node that contains the email(s) you want to delete (for example, select the **Today** node if you want to delete emails that were quarantined today). Alternatively, you can use Quick Search to look for the emails that you want to delete.

NOTE: You can delete an email that was quarantined today from the **Today** node, the **This Week** node, the **All Emails** node as well as from any Search Folder that contains the email. The difference between the mentioned nodes is the amount of emails that are present within.

2. Select the check box of the email(s) you want to delete and click **Delete items**.

NOTE 1: If you want to delete all the listed emails, you do not need to select all the check boxes individually. Just click **Delete all**.

NOTE 2: To refresh the information, click **Update**.

NOTE 3: If an email matches more than one search folder, the administrator does not need to delete the same email from each search folder. If you delete an email from a search folder, GFI MailSecurity removes it from the Quarantine Store and so it does not list in any of the other search folders.

Rescanning emails from the Quarantine Store

The Quarantine Store allows you to submit quarantined emails for rescanning. This option is provided mostly to cater for virus outbreak scenarios.

For example, an email is quarantined on Monday because it infringed a Content Checking rule. The same email also contained a newly released virus. However, since the virus signatures had not yet been updated when it passed through GFI MailSecurity, it did not infringe any virus scanning rules.

A few hours after this email was quarantined, the virus signatures are updated. The next day, the administrator comes across this email while going through the quarantine store. If rescanning of quarantined items was not possible, the administrator would have only two options, delete the email, or approve it and release a virus unknowingly.

With the rescan option, the administrator can choose to submit the email for rescanning. This time around, since the virus signatures were updated, the email will infringe both a virus scanner rule, as well as the same Content Checking rule.

When the administrator finds the same email in the Quarantine Store, the reason for quarantining will be that a virus was detected. The administrator will then most probably choose to delete the email.

To rescan emails from the Quarantine Store:

1. Expand the **GFI MailSecurity ► Quarantine** node and select the sub-node that contains the email(s) you want to rescan (for example, select the **Today** node if you want to rescan emails that were blocked today). Alternatively, you can use Quick Search to look for the emails that you want to rescan.

2. Select the check box of the email(s) you want to rescan and click **Rescan items**.

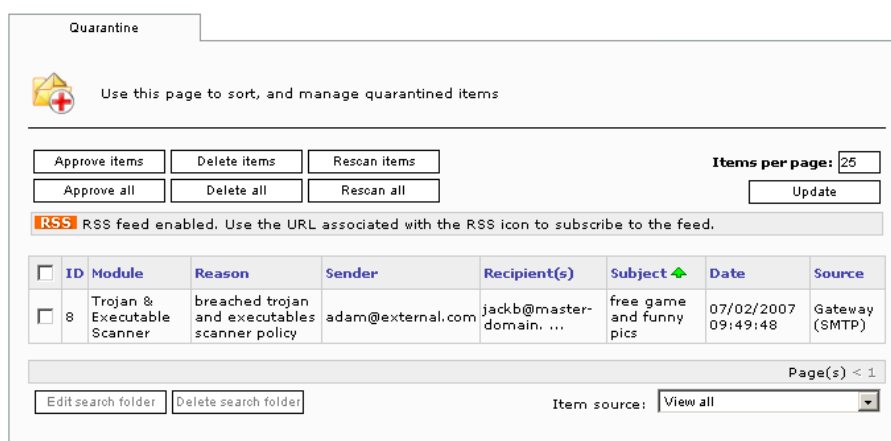
NOTE 1: If you want to rescan all the listed emails, you do not need to select all the check boxes individually. Just click **Rescan all**.

NOTE 2: To refresh the information, click **Update**.

View the full security threat report of an email

To view the full security threat report of a quarantined email, follow these steps:

1. Expand the **GFI MailSecurity ▶ Quarantine** node and select the sub-node that contains the email(s) you want to view (for example, select the **Today** node if you want to view emails that GFI MailSecurity quarantined today). Alternatively, you can use Quick Search to look for the emails that you want to view.
2. GFI MailSecurity lists the quarantined emails in a table. GFI MailSecurity can quarantine an email for one or more security reasons, but it only displays the top security threat under the **Reason** column.



The screenshot shows the 'Quarantine' page in GFI MailSecurity. It includes a header with a warning icon and the text 'Use this page to sort, and manage quarantined items'. Below this are buttons for 'Approve items', 'Delete items', 'Rescan items', 'Approve all', 'Delete all', 'Rescan all', and an 'Update' button. An 'RSS' feed icon and text are also present. A table lists quarantined items with columns: ID, Module, Reason, Sender, Recipient(s), Subject, Date, and Source. The table contains one row with ID 8, Module 'Trojan & Executable Scanner', Reason 'breached trojan and executables scanner policy', Sender 'adam@external.com', Recipient(s) 'jackb@master-domain. ...', Subject 'free game and funny pics', Date '07/02/2007 09:49:48', and Source 'Gateway (SMTP)'. At the bottom, there are buttons for 'Edit search folder' and 'Delete search folder', and a dropdown for 'Item source' set to 'View all'.

ID	Module	Reason	Sender	Recipient(s)	Subject	Date	Source
8	Trojan & Executable Scanner	breached trojan and executables scanner policy	adam@external.com	jackb@master-domain. ...	free game and funny pics	07/02/2007 09:49:48	Gateway (SMTP)

Screenshot 91 - A quarantined email

3. To view the full security threat report, click on the row of the quarantined email you want to view. GFI MailSecurity will list all the body parts of the email such as plain text body, HTML body, and any attachments.

4. To return to the list of quarantined emails, click **Back**.

NOTE 1: From this page you can also approve, delete, or re-scan the particular email you are currently viewing, by clicking the respective button. If you want to delete an email and inform the intended recipients of the action taken, click **Delete and Notify** instead of **Delete**.

NOTE 2: If you want to download the quarantined item, click **Download Item**.

NOTE 3: Unless the source of the item is **Information Store (VSAPI)**, you can approve a sanitized version of the email by clicking **Sanitize and Approve**. When you click this option, GFI MailSecurity removes the email from the quarantine store and sends it to the intended recipients, but before doing so, all the body parts that have a security threat are removed from the email, thus rendering it safe.

Quarantined email

Showing details for quarantined item 8

Approve

Sanitize and Approve

Rescan

Delete

Delete and Notify

Download item

Back

Item Information

Source:

Gateway (SMTP)

Subject:

Free game and funny pics

From:

adam@external.com

To:

jackb@master-domain.com

Date:

07/02/2007 09:49:48

Module:

Trojan & Executable Scanner

Scan Modules:

Trojan & Executable Scanner

Attachment Checking

Content Checking

Attachments

Filename (size)	Threat Description
coolgame.exe (1008Kb) ⓘ	Breached Trojan and Executables scanner policy
<div>Module</div> <div>Trojan & Executable Scanner</div>	File 'coolgame.exe' breached the following Trojan & Executable Scanner rule/s: "Checks if the executable tries to change keyboard, mouse or display settings (CheckUIChange)"
<div>Module</div> <div>Attachment Checking</div>	File "coolgame.exe" triggered rule "CONTENT POLICY: Block all potentially malicious attachments" (Claimed extension "exe" listed in "block" extension list)
fun 03.jpg (22.91Kb) ⓘ	Triggered rule "CONTENT POLICY: Block most common image attachments (.jpg, etc.)"
fun 04.gif (22.91Kb) ⓘ	Triggered rule "CONTENT POLICY: Block most common image attachments (.jpg, etc.)"
fun 02.jpg (22.91Kb) ⓘ	Triggered rule "CONTENT POLICY: Block most common image attachments (.jpg, etc.)"
<div>Module</div> <div>Attachment Checking</div>	File "fun 02.jpg" triggered rule "CONTENT POLICY: Block most common image attachments (.jpg, etc.)" (Claimed extension "jpg" listed in "block" extension list)
fun 01.jpg (22.91Kb) ⓘ	Triggered rule "CONTENT POLICY: Block most common image attachments (.jpg, etc.)"

Message Text

Text Body

HTML Body

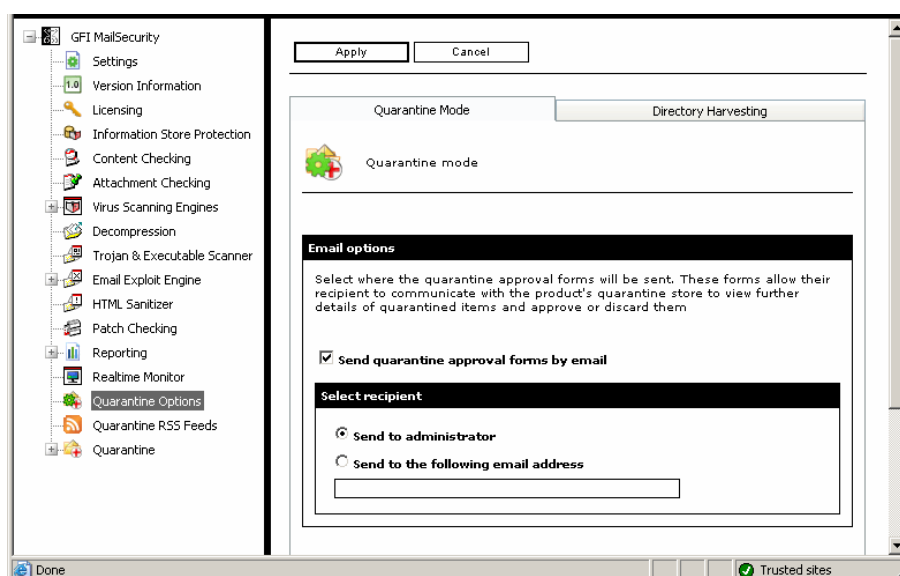
Please click here to see quarantined content

The message body might contain malicious content. Instead of displaying the message body, the threat description is being shown. The following table shows the threat details for this message body. To view the actual message body, please click the link above.

Plugin	Threat
Content Checking	Words in body triggered rule "CONTENT POLICY: Block Sexual Content" (Words found: jack)

Screenshot 92 - Viewing the full security threat report of a quarantined email

Enable email approval via HTML approval forms



Screenshot 93 - Quarantine Options configuration page

You can configure GFI MailSecurity to send HTML Quarantine Action Forms through email to the administrator or an authorized user. The Quarantine Action Form makes it possible for the administrator to approve or delete quarantined emails directly from the email client without accessing the Quarantine Store. To enable the sending of HTML Quarantine Action Forms, follow these steps:

1. Click the **GFI MailSecurity ► Quarantine Options** node.
2. Select the **Send quarantine approval forms by email** check box to enable the sending of HTML Quarantine Action Forms through email.
3. Specify to whom you want to send the HTML Quarantine Action Forms (i.e. specify who will review/approve the quarantined emails) by selecting one of the following options:
 - **Send to administrator** - Select this option to send the HTML Quarantine Action Forms to the administrator (i.e. using the email address specified during the installation stage or configured in the **GFI MailSecurity ► Settings node ► General tab**). For more information on how to configure the administrator's email address, refer to the 'Define the administrator's email address' section in the General Settings chapter.
 - **Send to the following email address** - Select this option to send the HTML Quarantine Action Forms to a specified email address/user group or public folder. Type the recipient in the box provided underneath this option.

NOTE: In the HTML Quarantine Action Form, you can click **More details** to view all the information related to the quarantined email.

4. Click **Apply**.

How to approve or delete quarantined emails from an email client

When GFI MailSecurity quarantines an email, the administrator receives an email containing an HTML Quarantine Action Form. The form contains details related to the quarantined email including the reason why it was blocked and any attachments that were included in the email.

http://win2k3entsvr - MSEC: jackb@master-domain.com, Attachment Checking, Triggered rule "CO...

Reply Reply to all Forward X Help

From: Administrator Sent: Mon 05/02/2007 15:07
To: Administrator
Cc:
Subject: MSEC: jackb@master-domain.com, Attachment Checking, Triggered rule "CONTENT POLICY: Block all potentially malicious attachments"

Attachments:

GFI MailSecurity Quarantine Action Form

Dear Administrator,

On the 05 February 2007 GFI MailSecurity quarantined the following item.

Item ID	7
Highest Priority Module	Attachment Checking
Subject	prank call
From	adam@external.com
To	jackb@master-domain.com

Threats detected

	Filename	Reason
	funny.mp3 (25B)	Attachment Checking : Triggered rule "CONTENT POLICY: Block all potentially malicious attachments"

Please select from the following options:

Unknown Zone (Mixed)

Screenshot 94 - HTML approval form

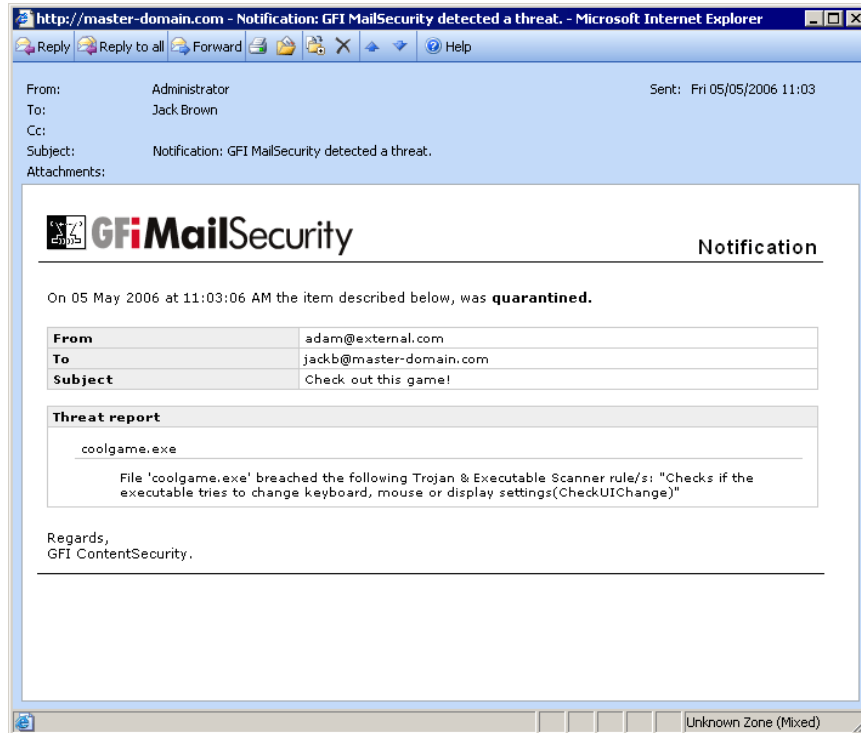
Through the HTML Quarantine Action Form, the administrator can approve or delete the email mentioned in the form by clicking on **Approve** or **Delete** accordingly. If the administrator approves the quarantined email, GFI MailSecurity will forward the quarantined email to the intended recipient and remove it from the Quarantine Store. In addition, if the email was inbound, the recipient will receive an email describing the status change of the quarantined email (i.e. approved or deleted). This email is mostly required to inform the user when the quarantined email is deleted.

Quarantined mail from the user point of view

The quarantining of mail is largely transparent to the mail user. For both inbound and outbound mail, users will receive the quarantined mail as soon as the administrator approves it.

If you select to notify the local user, via the notification options group under the actions tab of a particular node, the local user will receive an email to inform him that an email was quarantined as shown in the following screenshot.

NOTE: If a threat is detected in an outbound email, the recipients will receive the original email with the malicious parts removed. A security notice is attached to the email to inform the recipients what email parts were removed and for what reason. This behavior is always enabled and is not affected by the 'notify local users' setting.



Screenshot 95 - Quarantined email user notification

Enable quarantine RSS feeds

What is RSS?

Really Simple Syndication (RSS) is a protocol used by websites that update their content frequently, for example news sites, weblogs and so on, to inform end users of what is new or updated on the website.

The website publishes an XML file, called an RSS feed, that complies with the schema defined in the RSS standard. End users make use of a special application, called a feed reader or aggregator, to subscribe to the different RSS feeds. The aggregator reads the XML file from the URL specified when subscribing, parses the content and displays a list of updated articles. The entries usually include a summary of the article and a link to view the full article.

How does GFI MailSecurity use RSS?

The quarantine store is like a website that is updated frequently with new blocked content. To facilitate the work of the administrator in keeping an eye on the GFI MailSecurity quarantine store, RSS feeds can now be enabled on the quarantine folders.

If you enable RSS feeds on a quarantine folder, the administrator can use an RSS feed reader to subscribe to the quarantine folder RSS

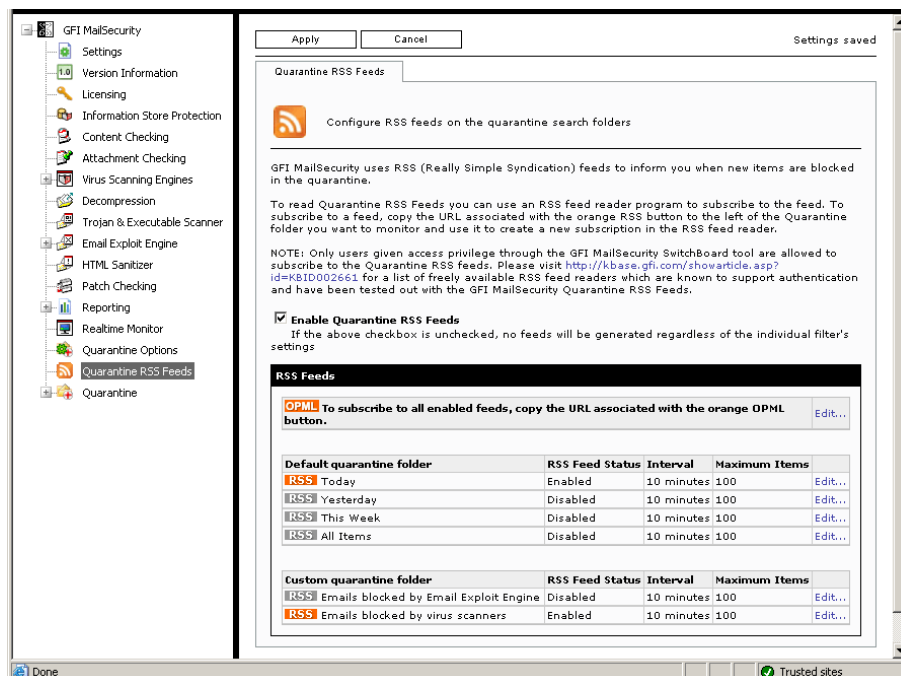
feed. Through the RSS feed reader, the administrator is periodically informed of new blocked content in the quarantine store.

NOTE: For a list of freely available RSS feed readers please visit <http://kbase.gfi.com/showarticle.asp?id=KBID002661>. The RSS feed readers listed support authentication and have been tested with the quarantine RSS feeds feature of GFI MailSecurity.

How do I configure RSS on a quarantine folder?

To enable RSS feeds on specific quarantine folders, follow these steps:

1. Click the **GFI MailSecurity ► Quarantine RSS Feeds** node.



Screenshot 96 - Quarantine RSS feeds

2. Select the **Enable Quarantine RSS Feeds** check box.
3. Under the **RSS Feeds** area you can view a list of all the quarantine search folders, both default and custom, currently configured. To configure RSS feeds for a particular quarantine folder, click **Edit** to the right of the quarantine folder entry.

RSS Feeds

OPML To subscribe to all enabled feeds, copy the URL associated with the orange OPML button. [Edit...](#)

Default quarantine folder	RSS Feed Status	Interval	Maximum Items
RSS Today	Enabled	10 minutes	100

☒ **Enable Quarantine RSS feeds on this folder**

Refresh feed content every:
 minutes

Feed should contain at most:
 items

Please use the following address to subscribe to this feed.

<http://WIN2K3ENTSVR80/MailSecurityRSS/rssfeed.aspx?feedName=today.xml&uniqueid=B6639C8A-B27E-403C-A63E-319C0>

NOTE: If you give everyone access to the RSS feeds from the GFI MailSecurity SwitchBoard application or disable NTLM security on the RSS feeds virtual directory, anyone will be able to subscribe to this feed. If you suspect unauthorized users managed to get a copy of this URL, click the 'Reset Feed URL' button to generate a new URL and click the 'Apply' button. You then need to modify the RSS subscription to point to the new URL.

^^^

RSS Yesterday	Disabled	10 minutes	100	Edit...
RSS This Week	Disabled	10 minutes	100	Edit...
RSS All Items	Disabled	10 minutes	100	Edit...

Custom quarantine folder	RSS Feed Status	Interval	Maximum Items
RSS Emails blocked by email exploit engine	Disabled	10 minutes	100
RSS Emails blocked by virus scanners	Enabled	10 minutes	100

Screenshot 97 - Quarantine folder RSS feed

4. Select the **Enable Quarantine RSS feeds on this folder** check box.

5. Specify an interval in minutes in the **Refresh feed content every** box. The default value is 10 minutes.

6. Specify the maximum number of items you want the feed to include in the **Feed should contain at most** box.

NOTE 1: By default, the GFI MailSecurity quarantine RSS feeds require authentication and thus only the users configured in the GFI MailSecurity SwitchBoard tool can subscribe to the RSS feeds. For more information, refer to the 'Securing access to the GFI MailSecurity Quarantine RSS feeds' section in the 'Installing GFI MailSecurity' chapter.

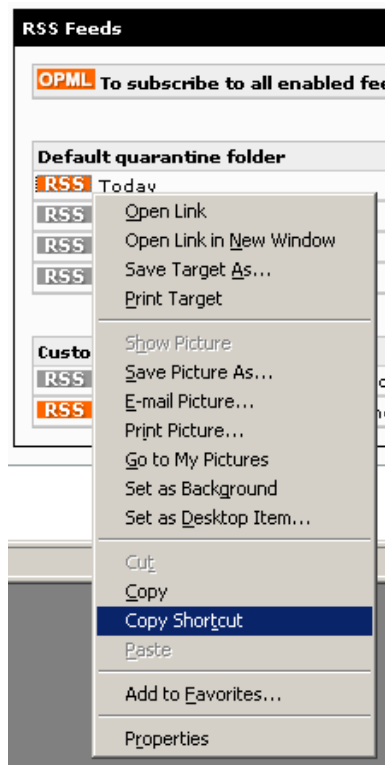
NOTE 2: If you give everyone access to the RSS feeds from the GFI MailSecurity SwitchBoard application or disable NTLM security on the RSS feeds virtual directory, anyone will be able to subscribe to the feeds. If you suspect unauthorized users managed to get a copy of a quarantine folder RSS feed URL, click the **Reset Feed URL** button for the specific quarantine folder and then click **Apply**. You then need to update the RSS subscription in your RSS feed reader application to point to the new URL. If you suspect that all RSS feed URLs might have been discovered, click **Edit** to the right of the **OPML** entry, click **Reset all the URLs** and then click **Apply**. You then need to update all the RSS subscriptions in your RSS feed reader to point to the new URLs.

7. Click **Apply**.

How do I subscribe to a quarantine search folder RSS feed?

To subscribe to an RSS feed follow these steps:

1. Right-click on the RSS icon to the left of the quarantine search folder to which you want to subscribe.



Screenshot 98 - Copy RSS feed URL

2. Click **Copy Shortcut**.

3. Use your favorite RSS feed reader application to create a new RSS feed subscription. Use the RSS feed URL copied in the previous step to specify the location of the feed.

NOTE: If you want to subscribe to all the enabled quarantine search folder RSS feeds in one go, copy the shortcut of the OPML icon. RSS feed reader applications usually have an option to import RSS feeds from an OPML file. An OPML file is an XML file that contains a list of RSS feeds, in this case all the quarantine search folder RSS feeds that are enabled.

Enable the Directory Harvesting filter on quarantined emails

Since GFI MailSecurity is usually installed as a first line of defense against email-based threats, it will process a lot of spam email because server level spam filters, such as GFI MailEssentials, are usually installed behind GFI MailSecurity.

For this reason, GFI MailSecurity will process a lot of spam email. Some of the spam email contains malicious attachments such as viruses, trojans and so on, and will thus be blocked by GFI MailSecurity and stored in the quarantine store for review.

Spam email quarantined by GFI MailSecurity will thus clutter the quarantine store with many useless emails, making the administrative review process more complex.

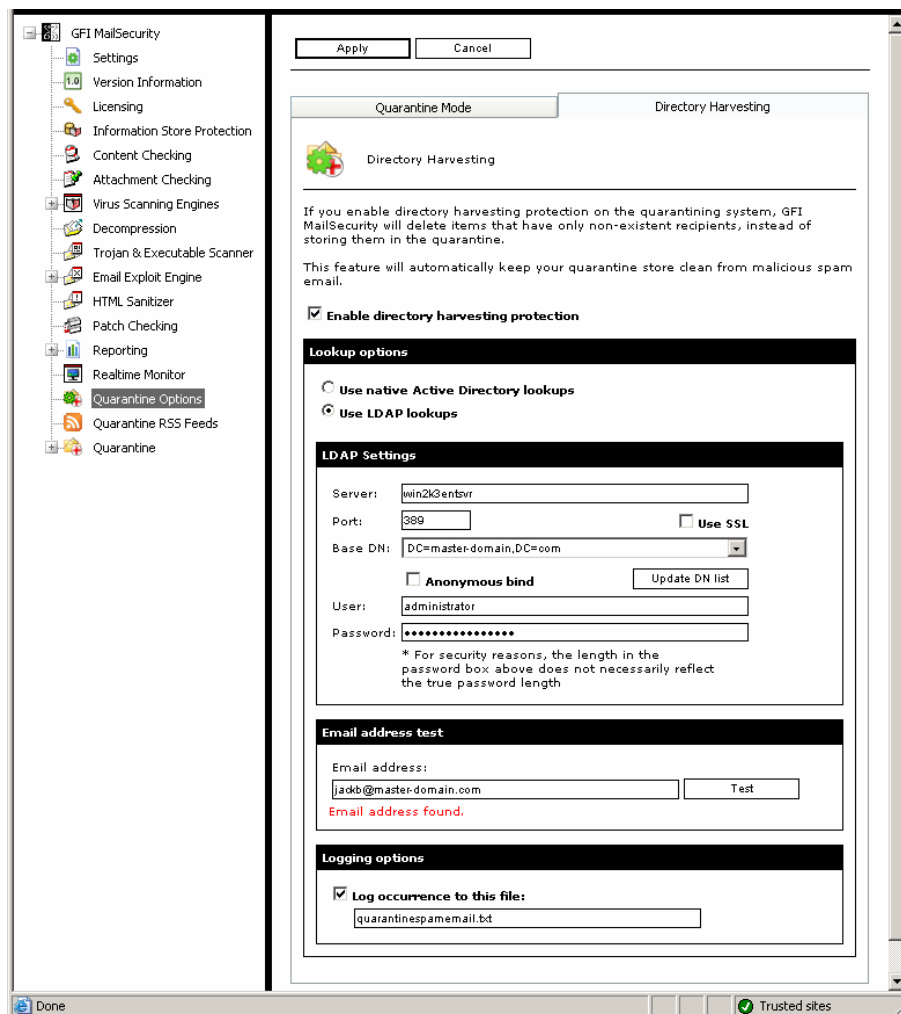
To eliminate malicious spam email from the quarantine store you can enable the Directory Harvesting filter on the quarantine store. The Directory Harvesting filter will scan emails that GFI MailSecurity blocks before they are stored in the quarantine store. If all the recipients of the blocked email are non-local or do not exist on the organizations

Active Directory or email server, GFI MailSecurity will delete the blocked email instead of storing it in the quarantine store.

The Directory Harvesting filter determines if a user exists or is local, by performing user lookups against the Active Directory or LDAP server you configure.

To enable the Directory Harvesting filter on the quarantine store, follow these steps:

1. Click the **GFI MailSecurity ► Quarantine Options** node.
2. Click the **Directory Harvesting** tab.



Screenshot 99 - Directory Harvesting filter

3. Select the **Enable directory harvesting protection** check box.
4. If you installed GFI MailSecurity in AD mode, click **Use native Active Directory lookups** and skip to step 7. If you want, you can choose to use LDAP lookups, as outlined in the next step.
5. If you installed GFI MailSecurity in SMTP mode, click **Use LDAP lookups**.
6. Specify the LDAP server name or IP in the **Server** box and the port number, default 389, in the **Port** box. If your LDAP server requires authentication, ensure that the **Anonymous bind** check box is clear and enter the authentication details in the **User** and **Password** boxes.

7. Click **Update DN list** to populate the **Base DN** list and select the appropriate entry from the list.

8. To test your LDAP configuration settings, specify a valid email address in the **Email address** box and click **Test**. If the lookup succeeds, **Email address found** is displayed underneath the **Email address** box.

NOTE 1: If you installed GFI MailSecurity in Active Directory user mode on a DMZ, the Active Directory of a DMZ normally does not include all the network users (i.e. email recipients) and as a result, you will be getting many false positives. In such cases, we recommend that you perform Directory Harvesting checks using LDAP lookups (i.e. click **Use LDAP lookups** and specify your LDAP server details).

NOTE 2: When GFI MailSecurity is setup behind a firewall, the Directory Harvesting feature will not be able to connect directly to the internal Active Directory because of the Firewall. In this case, although both options will be available, you must use LDAP lookups in order to enable the Directory Harvesting filter to connect to the internal Active Directory of your network (i.e., pass through your Firewall). Make sure to enable default port 389 on your Firewall

NOTE 3: When connecting to an Active Directory using LDAP (i.e. when GFI MailSecurity is installed on a DMZ or behind a Firewall), you have to specify the authentication credentials in this form: Domain\User (e.g. master-domain administrator).

NOTE 4: In an Active Directory, normally the LDAP server is the Domain Controller.

9. If you want to keep a log of the emails that GFI MailSecurity deletes through the Directory Harvesting filter, select the **Log occurrence to this file** check box and specify a log file name in the box below.

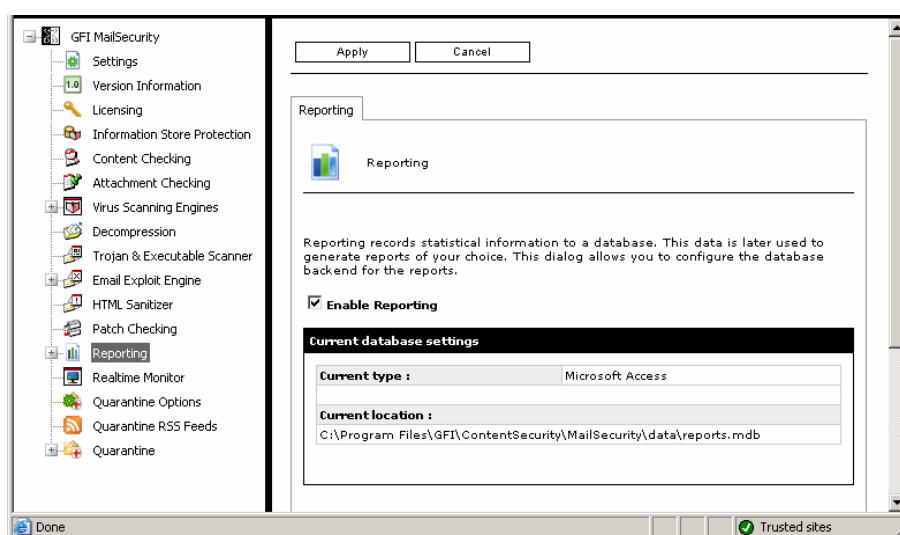
10. Click **Apply**.

Reporting

Introduction to GFI MailSecurity Reporting

Through the reporting option, you can configure GFI MailSecurity to log statistical data, such as the amount of emails being processed and quarantined, into a database. You can then buy the GFI MailSecurity ReportPack add-on, to generate informative reports based on the data collected in the database. For further information on the features included in the GFI MailSecurity ReportPack, refer to the GFI MailSecurity ReportPack chapters further on in this manual. GFI MailSecurity supports both Microsoft Access and Microsoft SQL Server as a database backend.

Configuring the statistical information database

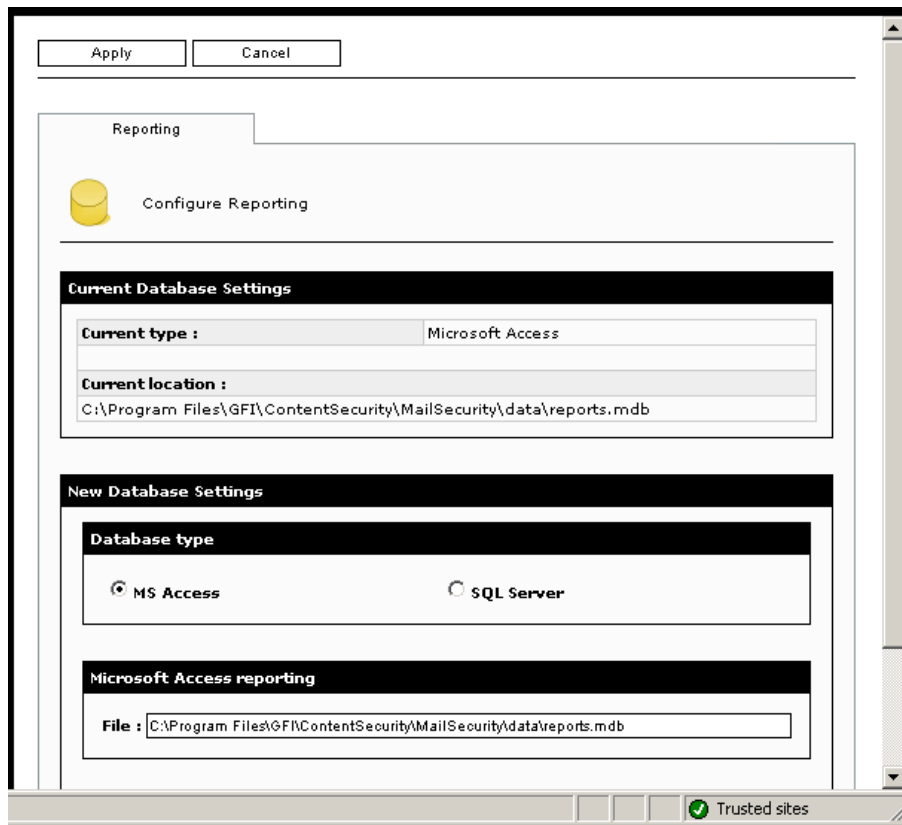


Screenshot 100 - Reporting page

To configure the reporting option:

1. Click the **GFI MailSecurity ► Reporting** node.
2. To enable data logging for reporting purposes, select the **Enable Reporting** check box. If clear this check box, no reporting data will be logged.
3. In the reporting page, you can see the details of the currently configured reporting database, such as the database type and the location of the database. To change the current database settings, expand the **Reporting** node and click the **Configure Database** sub-node.
4. In the Configure Reporting page, you can configure the reporting database as follows:

Configuring a Microsoft Access database backend



Screenshot 101 – Configuring a Microsoft Access database backend

1. Click **MS Access** and type the complete path including the filename of the database file in which the statistical data must be stored. If you only specify a filename, the database file is created in the default path i.e.

C:\Program Files\GFI\ContentSecurity\MailSecurity\data\
<filename.mdb>

2. Click **Apply**.

Configuring a Microsoft SQL Server database backend

The screenshot shows the 'Configure Reporting' window. At the top, there is a 'Reporting' tab and a 'Configure Reporting' button with a yellow cylinder icon. Below this, the 'Current Database Settings' section shows 'Current type' as 'Microsoft Access' and 'Current location' as 'C:\Program Files\GFI\ContentSecurity\MailSecurity\data\reports.mdb'. The 'New Database Settings' section has a 'Database type' section with radio buttons for 'MS Access' and 'SQL Server', where 'SQL Server' is selected. Below this is the 'SQL server reporting' section with radio buttons for 'Detected server' (selected) and 'Manually specified server'. The 'Detected server' dropdown shows '(local)'. There are input fields for 'User' (containing 'sa') and 'Password' (masked with dots). A 'Get Database List' button is next to the password field. The 'Database' dropdown shows 'GFI MailSecurity Reporting Database'.

Screenshot 102 - Configuring SQL Server Database backend

1. Click **SQL Server**.
2. Click **Detected server** and then select the SQL Server from the **Server** list or else click **Manually specified server** and in the box type the IP or server name where Microsoft SQL Server is hosted.
3. Type the name of a user that is authorized to access the Microsoft SQL Server in the **User** box.
4. Type the password for this account in the **Password** box.
5. Click **Get Database List** to extract the database information from this server and populate the **Database** list.
6. From the **Database** list, select the database where you want to store the statistical data.
7. Click **Apply**.

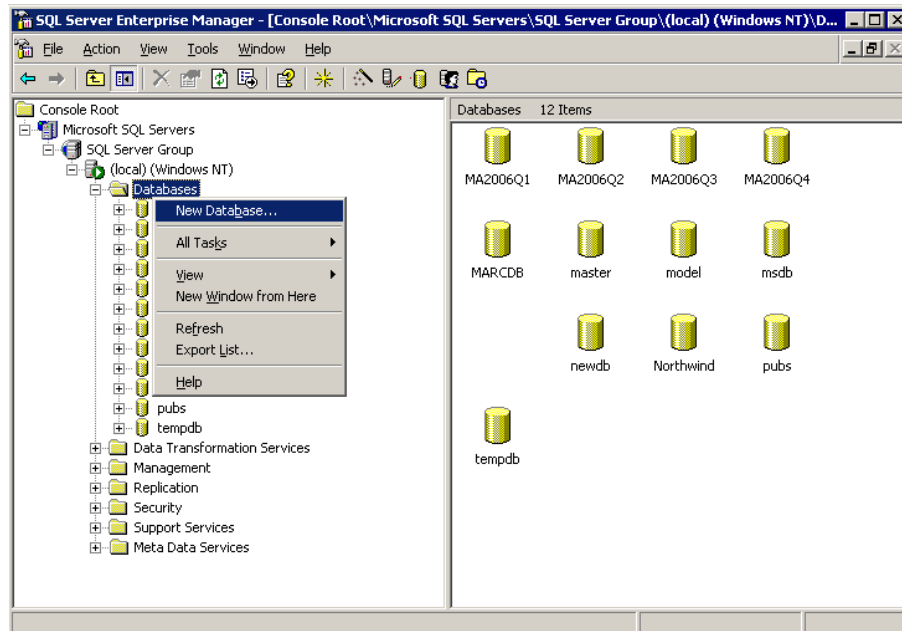
NOTE 1: Make sure that you have already created the database on Microsoft SQL Server before configuring this option. For more information on how to create a database on SQL Server, refer to the 'Creating a new database on Microsoft SQL Server' section below.

NOTE 2: The user and password you specify must be identical to the ones specified when creating the login account for your database on

Microsoft SQL Server. For more information, refer to step 6 in the 'Creating a new database on Microsoft SQL Server' section below.

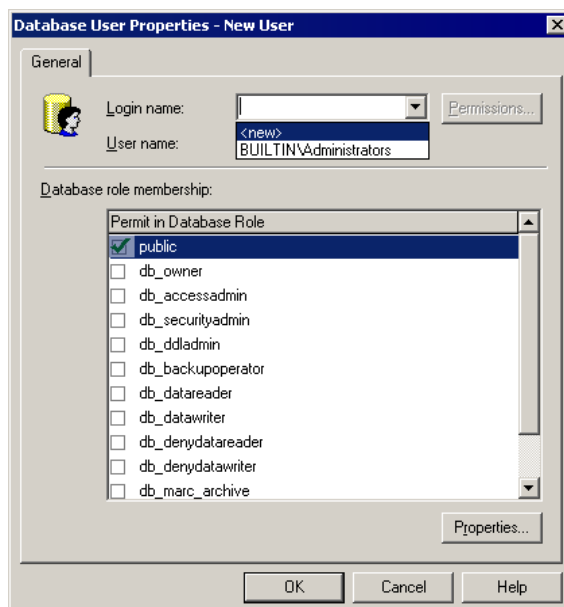
Creating a new database on Microsoft SQL Server

1. Open the SQL Server Enterprise Manager (**Start ► Programs ► Microsoft SQL Server ► Enterprise Manager**) and expand the Microsoft SQL Server node where you want to create the database.



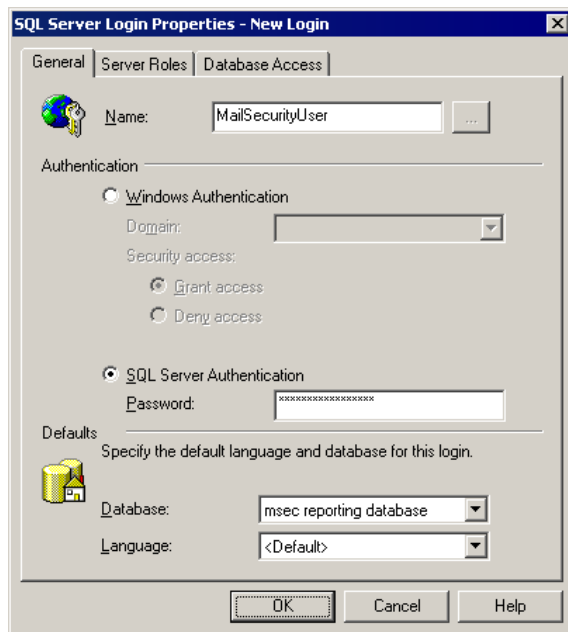
Screenshot 103 - Creating a new database

2. Right-Click the **Databases** node and then click **New Database**.
3. Type the database name in the dialog box, for example, 'MailSecurityReports', and then click **OK**.
4. Expand the newly created database node, right-click the **Users** sub-node and then click **New Database User**.



Screenshot 104 - Creating a login

5. From the **Login name** list, select **<new>**.



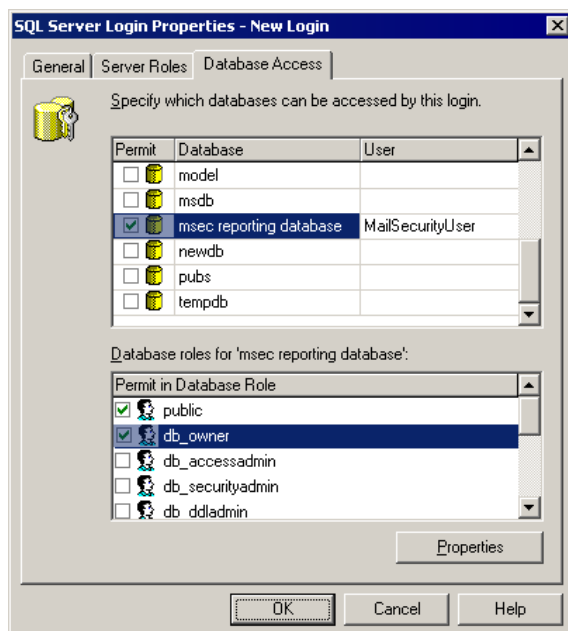
Screenshot 105 - Specifying authentication mode

6. In the **SQL Server Login Properties** dialog box, type the login name, for example, 'MailSecurityUser', in the **Name** box. Under the **Authentication** area, click **SQL Server Authentication** and then type a password in the **Password** box.

7. Select the database you have just created from the **Database** list.

8. Click the **Database Access** tab.

9. Select the check box near the Database you have just created.



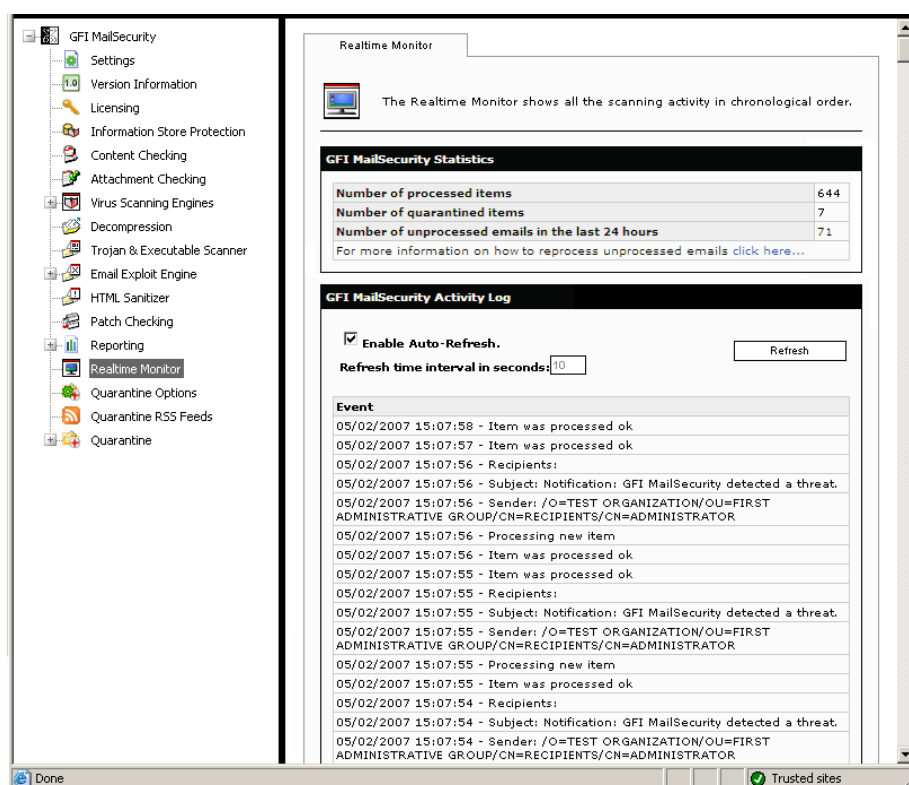
Screenshot 106 - Enabling the db_owner field

10. In the **Database roles for** list, select **db_owner**. Click **OK** to save your settings.

Realtime Monitor

About the Realtime Monitor

Through the Realtime Monitor page, you can monitor the GFI MailSecurity email processing activity in a 'Live' environment. Therefore, you can use this option to check the status of each email and determine whether an email was successfully processed, not processed or quarantined.



Screenshot 107 - Realtime Monitor page

Monitoring email activity

Click the **GFI MailSecurity ► Realtime Monitor** node to open the Realtime Monitor page. This page displays the GFI MailSecurity email statistics and event log.

The GFI MailSecurity Statistics area shows the:

- **Number of processed items** – number of emails which were successfully scanned by the product.
- **Number of quarantined items** – number of emails which were directed to quarantine.

- **Number of unprocessed emails in the last 24 hours** – number of emails that are not processed by GFI MailSecurity and not delivered to the recipient. One reason this can happen is when the email is corrupted spam and therefore could not be processed successfully. A copy of these emails can be found at <..\GFI\Content Security\MailSecurity\FailedMails> folder.

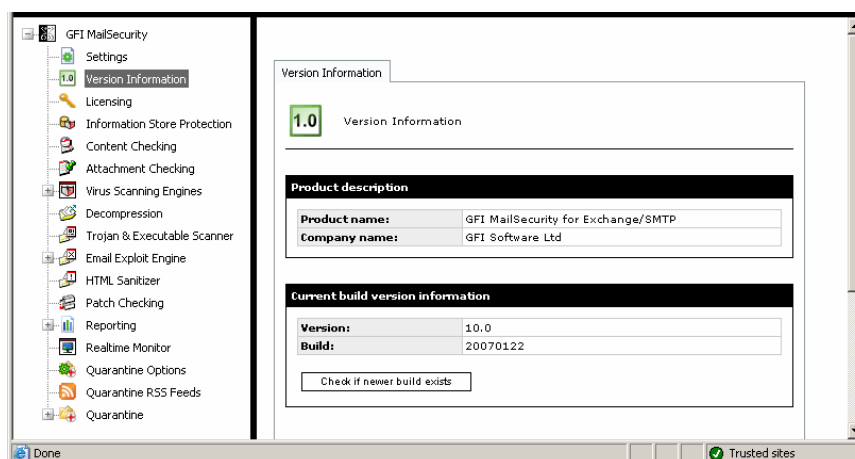
NOTE: For more information about unprocessed emails refer to: <http://kbase.gfi.com/showarticle.asp?id=KBID003263>

In the GFI MailSecurity Activity Log select the **Enable Auto-Refresh** check box and specify a time interval in seconds for automatic refresh of the Realtime Monitor. Alternatively, click on **Refresh** to refresh the activity manually.

In the **Event** area, the page displays the date and time when GFI MailSecurity receives and scans an email, as well as the sender, recipient and subject of every email scanned.

Miscellaneous

Version Information



Screenshot 108 - Version Information page

To view the GFI MailSecurity version information, click the **GFI MailSecurity ► Version Information** node. The version information page displays the GFI MailSecurity version number currently installed and the build information. To check whether you have the latest build of GFI MailSecurity installed on your machine, click **Check if newer build exists**.

NOTE: Please, always quote your GFI product Version and Build information when requesting for GFI support.

Additional Copyright Information

Some components of GFI MailSecurity have been created using software developed by third-party software developers. Their software license information is included below.

Libxml2: The MIT License

Copyright (C) 1998-2003 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL DANIEL VEILLARD BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of Daniel Veillard shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

Advanced topics

Customizing the notification templates

GFI MailSecurity sends notification emails to the administrator/user whenever an event that needs attention occurs.

There are two types of notifications:

- **Administrative notifications** – GFI MailSecurity sends these notifications, for example, when a license is going to expire, when a new patch is available, and when new anti-virus engine updates are available.
- **End user notifications** – GFI MailSecurity sends these notifications to the sender/recipient of an email when an email gets quarantined or modified.

The notification email message is generated from templates stored in sub-folders in the `ContentSecurity\MailSecurity\Templates` folder.

Each template sub-folder can contain an HTML body template (`html.txt`), a text body template (`text.txt`), and a subject template (`subject.txt`).

NOTE: The template folder names and template file names are predefined and therefore you cannot change them.

The templates contain the text of the notification message, as well as field names that are replaced by dynamic values upon generation of the notification message.

There are two types of template:

- **Tag-based templates** – These templates use tags (in the form "[TAGNAME]") to indicate fields which need to be replaced with dynamic data.
- **XSL-based templates** – These templates are an XSL style sheet, and are used in conjunction with dynamically created XML data to generate the notification message.

NOTE: Always take a backup of the template you are going to modify. In this way, you can always recover from the backup template if your modified template does not work as expected.

NOTE: Before modifying XSL-based templates, make sure you are proficient in XML and XSL. If you modify an XSL template and it is not well formed, for example, the notification services module will fail to send notification emails. To check whether an XSL based template is well formed, you can rename the template filename with an extension of ".xml" and load it in Microsoft Internet Explorer. If the template is well formed, the browser will load it correctly. If it contains errors, the browser will highlight the exact line where the problem is located.

Variables used in XSL-based notification templates

Notify user and notify manager notifications (in notifyuser folder and notifymanager folder respectively)

Node	Description
"itemsenderemailaddress"	The sender's email address.
"itemsubject"	The quarantined email subject.
"itemdeliverytime"	The date and time the message was delivered.
"itemrecipients/recipient"	The message recipients. Use xsl:for-each to enumerate.
"action"	Action taken on message by GFI MailSecurity.
"shortdate"	Date when email was processed. Short date format.
"longdate"	Date when email was processed. Long date format.
"time24"	Time when email was processed. 24 hour format.
"time12"	Time when email was processed.
"infringedrules/rule"	List of rules infringed. Use xsl:for-each to enumerate.
"itemmessageid"	The message ID of the email processed.
"itemscandirection"	0 – Inbound : 1 – Outbound : 4 – Mixed

The listing on the next page shows a typical notify manager XSL template, which will generate the following HTML output.

HTML Output

```
<HTML>
<BODY>
On 04 August 2005 an email was blocked which has violated the following
rules:<P></P>
<B>BitDefender Anti-Virus</B><BR/>
<P>
The following action(s) were taken: <B>Quarantined</B>
</P>
Additional information:
<P>
<table border="1">
<tr>
<td>Subject</td><td><B>Sample email subject</B></td>
</tr>
<tr>
<td>Sender</td><td><B>samplesender@sampldomain.com</B></td>
</tr>
<tr>
<td colspan="2" align="center">Recipients</td>
</tr>
<tr>
<td colspan="2"><B>samplerrecipient@localdomain.com</B></td>
</tr>
</table>
</P>
Regards,<BR/>
GFI ContentSecurity.
</BODY>
</HTML>
```

XSL Template

```
<?xml version="1.0"?>
<xsl:stylesheet
    xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
    version="1.0">
<xsl:output method="html" omit-xml-declaration="yes" standalone="no"/>

<xsl:template match="/properties">
<HTML>
<BODY>

On <xsl:value-of select="longdate"/> an email was blocked which has
violated the following rules:<P/>
<xsl:for-each select="infringedrules/rule">
<B><xsl:value-of select="."/></B><BR/>
</xsl:for-each>

<P>
The following action(s) were taken: <B><xsl:value-of
select="action"/></B>
</P>

Additional information:

<P>
<table border="1">
<tr>
<td>Subject</td>
<td><B><xsl:value-of select="itemssubject"/></B></td>
</tr>
<tr>
<td>Sender</td>
<td><B><xsl:value-of select="itemsenderemailaddress"/></B></td>
</tr>
<tr>
<td colspan="2" align="center">Recipients</td>
</tr>

<xsl:for-each select="itemrecipients/recipient">
<tr>
<td colspan="2"><B><xsl:value-of select="."/></B></td>
</tr>
</xsl:for-each>
</table>
</P>

Regards,<BR/>
GFI ContentSecurity.
</BODY>
</HTML>
</xsl:template>

</xsl:stylesheet>
```

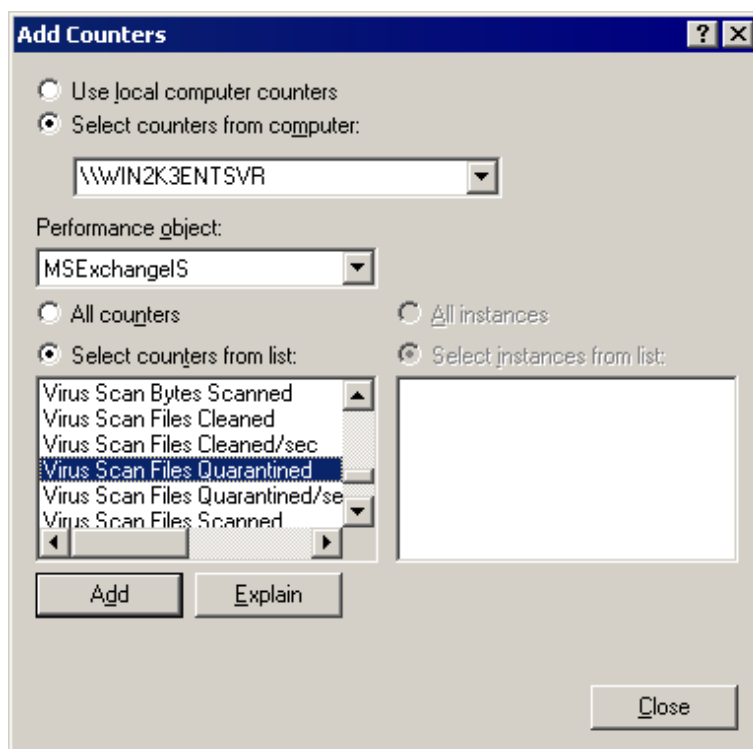
Setting Virus Scanning API Performance Monitor Counters

When you install GFI MailSecurity on the Microsoft Exchange machine directly, you can use the Performance Monitor MMC to keep an eye on Virus Scanning API performance through the performance monitor counters made available by Microsoft Exchange.

NOTE: The VSAPI performance monitor counters are only available on a Microsoft Exchange Server 2007 machine with the Mailbox Server Role installed.

To add and view, the performance monitor counters listed below, follow these steps:

1. Click on **Start ► Control Panel**.
2. In the **Control Panel** window, double-click **Administrative Tools**.
3. In the **Administrative Tools** window, double-click **Performance**, to start the Performance monitor MMC.
4. Press Ctrl+I to load the **Add Counters** dialog box.
5. From the **Performance object** list, select **MSExchangeIS**.
6. Click **Select counters from list**.
7. Select one of the **Virus Scan** counters as listed below.
8. Click **Add**.
9. Repeat step 7 and 8 to add all the performance counters you want.
10. Click **Close**.



Screenshot 109 - Adding VSAPI performance monitor counters

The information provided below is also available from the following link: <http://support.microsoft.com/kb/285696>

The following VSAPI Performance Monitor counters are available:

Virus Scan Messages Processed – This is a cumulative value of the total number of top-level messages that are processed by the virus scanner.

Virus Scan Messages Processed/sec – This counter represents the rate at which top-level messages are processed by the virus scanner.

Virus Scan Messages Cleaned – The total number of top-level messages that are cleaned by the virus scanner.

Virus Scan Messages Cleaned/sec – The rate at which top-level messages are cleaned by the virus scanner.

Virus Scan Messages Quarantined – The total number of top-level messages that are put into quarantine by the virus scanner.

Virus Scan Messages Quarantined/sec – The rate at which top-level messages are put into quarantine by the virus scanner.

Virus Scan Files Scanned – The total number of separate files that are processed by the virus scanner.

Virus Scan Files Scanned/sec – The rate at which separate files are processed by the virus scanner.

Virus Scan Files Cleaned – The total number of separate files that are cleaned by the virus scanner.

Virus Scan Files Cleaned/sec – The rate at which separate files are cleaned by the virus scanner.

Virus Scan Files Quarantined – The total number of separate files that are put into quarantine by the virus scanner.

Virus Scan Files Quarantined/sec – The rate at which separate files are put into quarantine by the virus scanner.

Virus Scan Bytes Scanned – The total number of bytes in all of the files that are processed by the virus scanner.

Virus Scan Queue Length – The current number of outstanding requests that are queued for virus scanning.

Virus Scan Folders Scanned in Background – The total number of folders that are processed by background scanning.

Virus Scan Messages Scanned in Background – The total number of messages that are processed by background scanning.

Troubleshooting

Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

- The manual – most issues can be solved by reading this manual.
- GFI Knowledge Base articles
- Web forum
- Contacting GFI Technical Support

Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit <http://kbase.gfi.com/>.

Web Forum

User to user technical support is available via the web forum. The forum can be found at: <http://forums.gfi.com/>.

Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online:** Fill out the support request form on: <http://support.gfi.com/supportrequestform.asp>. Follow the instructions on this page closely to submit your support request.
- **Phone:** To obtain the correct technical support phone number for your region please visit: <http://www.gfi.com/company/contact.htm>.

NOTE: Before you contact our Technical Support team, please have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at: <http://customers.gfi.com>.

We will answer your query within 24 hours or less, depending on your time zone.

Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit:
<http://www.gfi.com/pages/productmailing.htm>.

GFI MailSecurity ReportPack - Introduction

About GFI ReportCenter

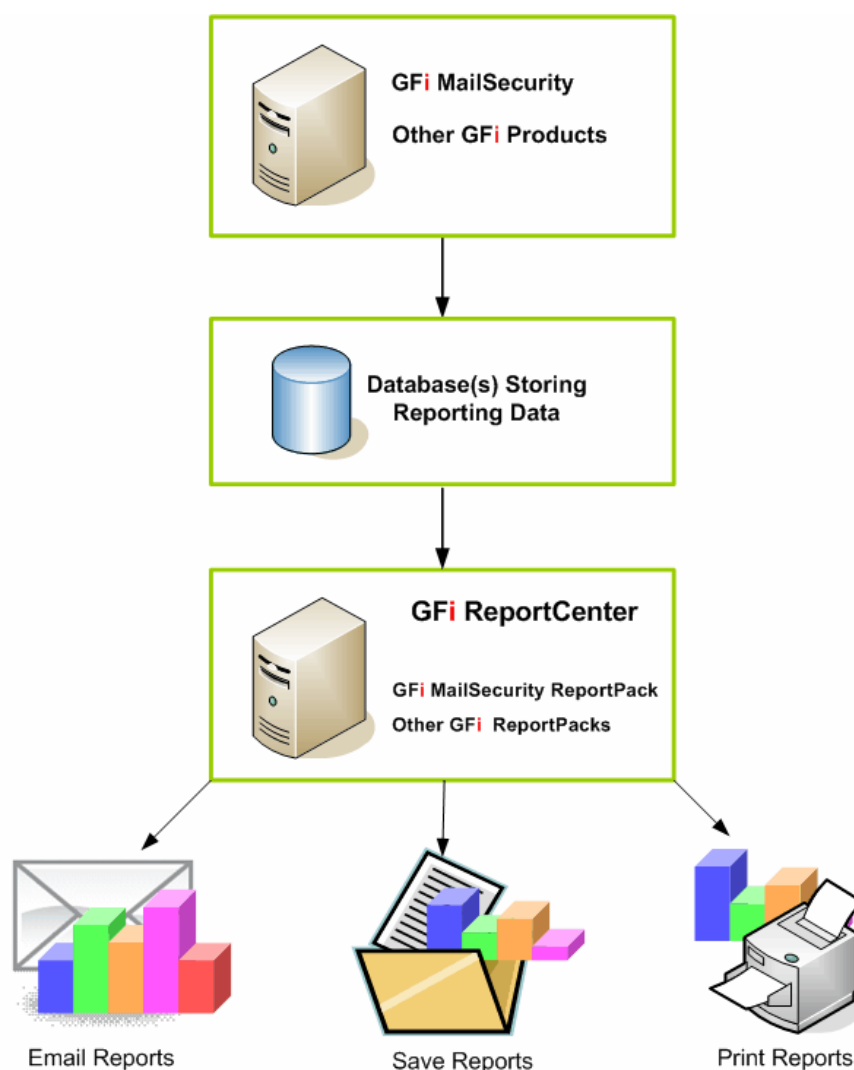


Figure 4 – GFI ReportCenter is a centralized reporting framework

GFI ReportCenter is a centralized reporting framework that utilizes the installed product ReportPacks to provide you with a list of available reports that you can generate. The information contained in the report is based on the data collected by the specific GFI product.

A ReportPack is thus a plug-in for GFI ReportCenter that exposes a set of reports that are useful for a particular GFI product. A ReportPack can be purchased as an add-on to the GFI product. An

example of a ReportPack is the GFI MailSecurity 10.0 ReportPack, further described in the following section.

About the GFI MailSecurity 10.0 ReportPack

The GFI MailSecurity 10.0 ReportPack is a full-fledged reporting companion to GFI MailSecurity. With the GFI MailSecurity 10.0 ReportPack, you can generate concise executive reports and detailed administrative reports.

From graphical traffic pattern reports for management, to tabular daily processed emails vs. blocked emails reports for technical staff, the GFI MailSecurity 10.0 ReportPack generates uncluttered reports that are simple yet highly effective. The reports provide you with the information you require to keep an eye on the GFI MailSecurity installation and the mail server.

The GFI MailSecurity 10.0 ReportPack allows for the creation of various graphical and text based reports showing:

- Inbound email Traffic
- Outbound email Traffic
- Viruses blocked
- Security threats blocked
- Virus outbreak trends
- Security threats outbreak patterns
- Mail server load patterns

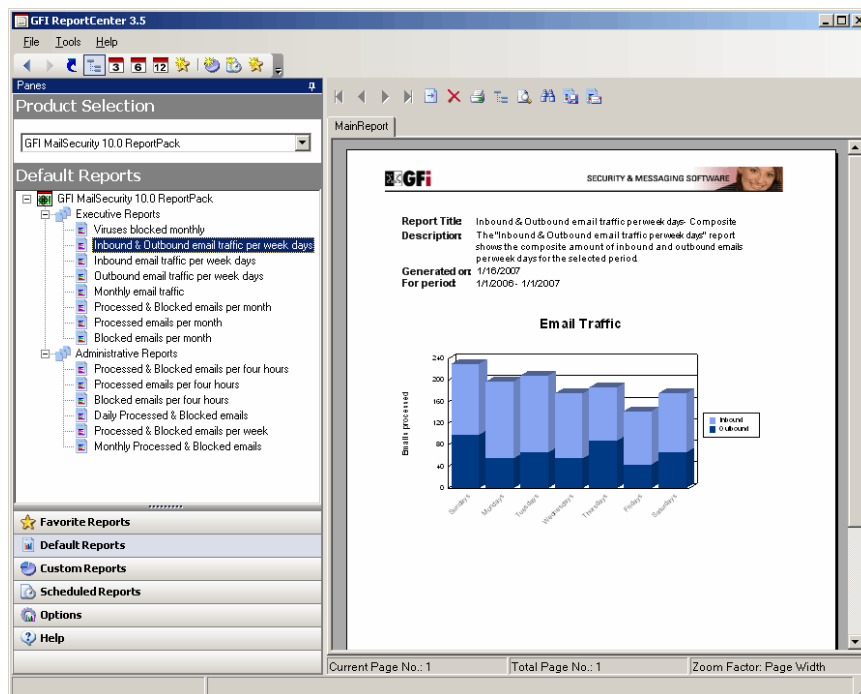
Components of the GFI MailSecurity 10.0 ReportPack

When you install the GFI MailSecurity 10.0 ReportPack, the following components are installed:

- GFI ReportCenter framework
- GFI MailSecurity 10.0 default reports
- Report scheduling service

GFI ReportCenter framework

The GFI ReportCenter framework is the management console through which you can navigate, generate, customize and schedule the reports included in the GFI MailSecurity 10.0 ReportPack. If you have other GFI products' ReportPacks installed on the same machine, you can use the GFI ReportCenter to make use of those reports as well.






Screenshot 110 - The GFI ReportCenter management console

The GFI ReportCenter management console is split into two panes, the navigation panel to the left of the screen, and the report-viewing pane to the right.

The navigation panel consists of the **Product Selection** list, from where you can select the GFI product ReportPack you want to use, and various panels, as outlined below, through which you can access all the features of GFI ReportCenter.

- Click on the **Default Reports** panel button to access the default list of reports that can be generated for the selected product. For more information on default reports refer to the 'GFI MailSecurity 10 default reports' section in this manual.
- Click on the **Favorite Report** panel button to access your favorite/most used reports. For more information on how to add reports to this list refer to the 'Adding default reports to the list of favorite reports' and 'Adding custom reports to the list of favorite reports' sections in this manual.
- Click on the **Custom Reports** panel button to access the list of customized reports you created for the selected product. For more information on how to create custom reports refer to the 'Custom reports' chapter in this manual.
- Click on the **Scheduled Reports** panel button to access the list of scheduled reports you created. For more information on how to create scheduled reports refer to the 'Scheduling reports' chapter in this manual.
- Click on the **Options** panel button to access the general configuration settings for the GFI product ReportPack selected in the Product Selection list.

- Click on the  **Help** panel button to view the quick reference guide in the report pane of the GFI ReportCenter management console.

In the report-viewing pane, you can view and analyze generated reports, maintain the list of scheduled reports, and explore the samples and descriptions of the default reports. When a report is generated, you can click on the  button to save the report to disk in various formats, such as HTML, Adobe Acrobat (PDF), Microsoft Excel (XLS), Microsoft Word (DOC), and Rich Text Format (RTF). If you want to send the generated report to someone by email, click on the  button.

GFI MailSecurity 10.0 default reports

The GFI MailSecurity 10.0 default reports are a collection of pre-configured reports that plug into the GFI ReportCenter framework. The default reports included in the GFI MailSecurity 10.0 ReportPack are split into two groups, executive reports and administrative reports. Default reports can also serve as the base template for the creation of customized reports that fit specific date ranges.

Report scheduling service

The report scheduling service controls the scheduling and automatic generation and distribution of reports. You can select in which output format you want the scheduling service to generate the reports. A variety of formats are available, such as DOC, PDF, RTF and HTML. You can also configure the scheduled report to do automatically one of the following once the report is generated: send the report by email, save on a disk, or both.

Key features

Centralized reporting

GFI ReportCenter is a one-stop, centralized reporting framework, which enables the generation and customization of graphical and tabular reports for a wide array of GFI Products.

Default reports

The GFI MailSecurity 10.0 ReportPack ships with a default set of graphical and tabular reports. These reports can be generated immediately after the installation, without any further configuration effort. The default reports in the GFI MailSecurity 10.0 ReportPack are organized into two different report-type categories:

- Executive Reports
- Administrative Reports

Distribution of reports via email

With GFI ReportCenter, you can distribute reports by email. You can also configure scheduled reports to be automatically distributed by email when generated.

Report export to various formats

By default, GFI ReportCenter allows you to export reports to various formats. Supported formats include HTML, PDF, XLS, DOC and RTF. You can configure a preferred report output format to be used as a default output format for scheduled reports. When creating or editing a scheduled report, you can choose to use the default output format, or else select another output format for the specific scheduled report.

Printing

All the reports generated by GFI ReportCenter are printer friendly and can be easily printed by clicking the  button on top of the report-viewing pane.

Report scheduling

With GFI ReportCenter, you can schedule reports to be generated on a pre-defined schedule as well as at specified intervals. For example, you can schedule lengthy reports to be generated after office hours. This allows you to maximize the availability of your system resources during working hours and avoid any possible disruptions to workflow.

Report customization

The default reports that ship with every ReportPack can serve as the base template for the creation of customized reports. You can customize a report by configuring a fixed or variable date range.

Favorites

GFI ReportCenter allows you to create bookmarks to your most frequently used reports – both default and custom.

Wizard assisted configuration

Wizards are provided to assist you in the configuration, scheduling and customization of reports.

License scheme and evaluation period

Evaluation period

All GFI ReportCenter features can be used during the evaluation period. The default evaluation period for this product is of 10 days. However, you can apply for a 30-day product evaluation key by filling in the online registration form on the GFI website (<http://www.gfi.com/downloads/register.aspx?pid=msec&vid=10-32&lid=en>) when downloading the product. This will also qualify you for free email support. After you download the product, you will receive an email containing a 30-day evaluation license key.

Purchasing a license key

You can purchase a license key online by visiting the GFI website (<https://www.gfi.com/pages/cart/orderform.aspx>). To license the product, you do not need to re-install the GFI ReportCenter framework and GFI MailSecurity 10.0 ReportPack. You only need to type the license key in the **Licensing** node provided in the management

console. For more information, refer to the 'Entering your license key after installation' section in this manual.

GFI MailSecurity ReportPack - Installation

System requirements

Install the GFI MailSecurity 10.0 ReportPack on a computer that meets the following requirements:

- Windows 2000 (SP4) / XP (SP2) / 2003 operating system
- Internet Explorer 6 or higher
- .NET Framework version 1.1.

Installation procedure

The GFI MailSecurity 10.0 ReportPack installation wizard will perform the following operations during the installation process.

- Verify that you are running the latest version of the GFI ReportCenter framework. If you are installing the framework for the first time or the currently installed framework version is outdated, the installation wizard will automatically download the latest one for you.
- Automatically install all the required components including the GFI ReportCenter framework, the GFI MailSecurity 10.0 ReportPack default reports and the Report Scheduling service.

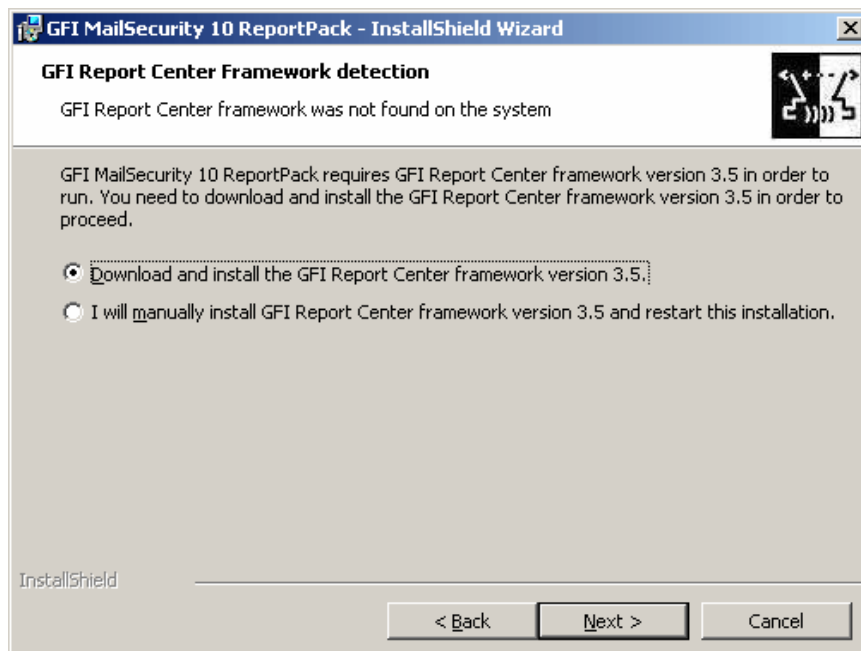
To install the GFI MailSecurity 10.0 ReportPack, follow these steps:

1. Double-click on **MSEC10ReportPack.exe**.



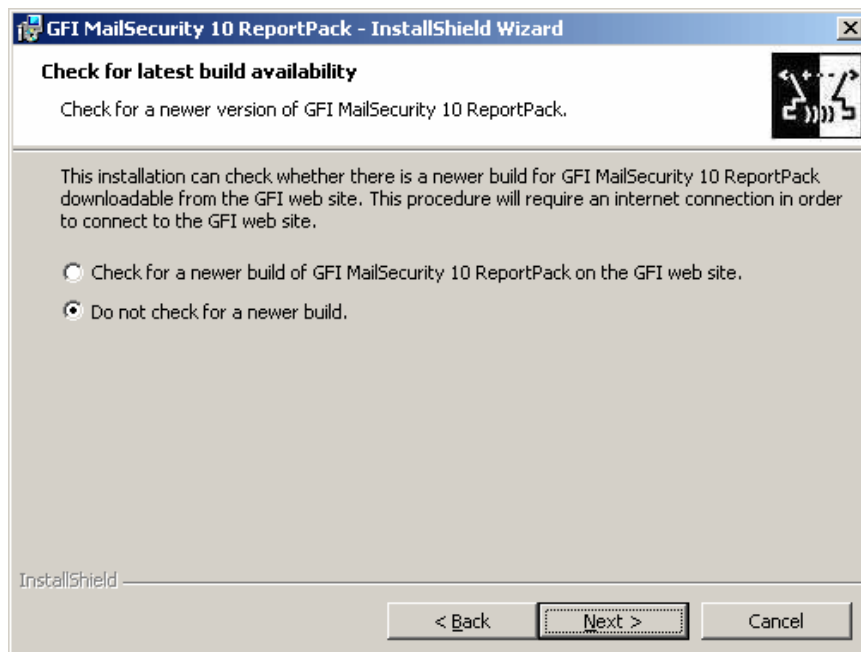
Screenshot 111 - Installation welcome page

2. In the welcome page, click **Next** to continue the installation.



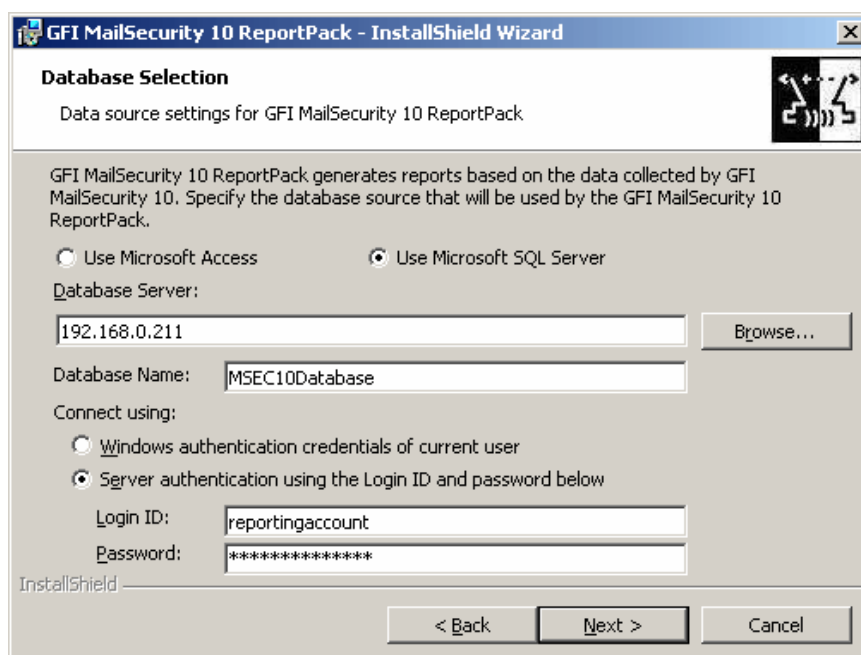
Screenshot 112 - GFI ReportCenter framework detection dialog

3. If the current version of your GFI ReportCenter framework is not compatible with the GFI MailSecurity 10.0 ReportPack, you will be prompted to download and install an updated version. To download the latest version of the GFI ReportCenter automatically, leave the dialog options as default and click **Next**.



Screenshot 113 - Check for a more recent build of the GFI MailSecurity 10.0 ReportPack

4. Choose whether you want the installation wizard to search for a newer build of the GFI MailSecurity 10.0 ReportPack on the GFI website. Then, click **Next** to proceed with the installation.
5. In the license page, read the licensing agreement carefully and then click **I accept the terms in the license agreement**. Click **Next** to continue.
6. Enter your Name, Company, and License key. If you are evaluating the product, leave the license key as default (i.e. **Evaluation**). Click **Next** to continue.



Screenshot 114 – Database selection page

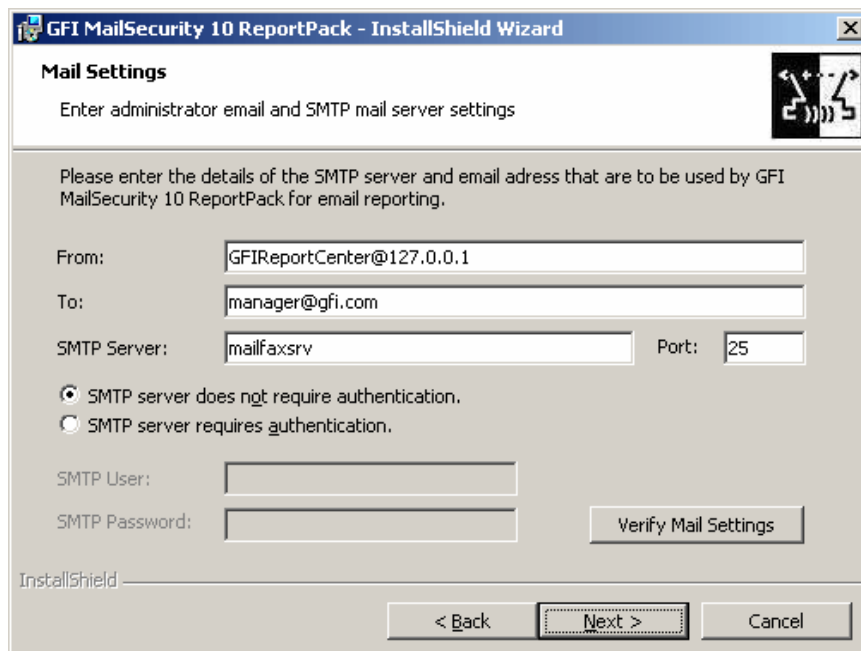
7. In the **Database Selection** page, you need to select the database you configured GFI MailSecurity to use for reporting purposes.

If you configured GFI MailSecurity to log reporting data into a Microsoft Access database, click **Use Microsoft Access** and then specify the full path in the **Database Path** box.

If on the other hand, you configured GFI MailSecurity to log reporting data into a Microsoft SQL Server database, click **Use Microsoft SQL Server** and then specify the server name or IP number of the machine hosting the Microsoft SQL Server in the **Database Server** box. In the **Database Name** box, specify the database containing the GFI MailSecurity reporting data. Select the authentication method you want to use to connect to the Microsoft SQL Server database. If you select **Server authentication** you need to specify a login name and password in the **Login ID** and **Password** boxes respectively.

NOTE: After the installation is complete, you can change the reporting database used by GFI ReportCenter at any time from the **Options** panel.

Click **Next** to continue.

The screenshot shows a Windows-style installation wizard window titled "GFI MailSecurity 10 ReportPack - InstallShield Wizard". The main heading is "Mail Settings" with a subtitle "Enter administrator email and SMTP mail server settings". Below this, a text box says "Please enter the details of the SMTP server and email address that are to be used by GFI MailSecurity 10 ReportPack for email reporting." The form contains several input fields: "From:" with the value "GFIReportCenter@127.0.0.1", "To:" with "manager@gfi.com", "SMTP Server:" with "mailfaxsrv", and "Port:" with "25". There are two radio buttons for authentication: "SMTP server does not require authentication." (which is selected) and "SMTP server requires authentication.". Below these are fields for "SMTP User:" and "SMTP Password:". A "Verify Mail Settings" button is located to the right of the password field. At the bottom, there are navigation buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel". The "InstallShield" logo is visible in the bottom left corner of the window.

Screenshot 115 - Email settings page

8. Specify the default email settings that you want GFI ReportCenter to use when sending reports by email. When you generate a report or while configuring a scheduled report, you can either use these default settings or else specify different settings for that specific report only. To check the email settings specified, you can click **Verify Mail Settings**. The installation wizard will send a test email to the address in the **To** box, using the SMTP server specified.

NOTE: After the installation is complete, you can change the email settings used by GFI ReportCenter at any time from the **Options** panel.

Click **Next** to continue.

9. Specify the product installation path or click **Next** to leave as default. The installation needs approximately 100 MB of free disk space.

10. The installation wizard is now ready to copy the required files and finalize the installation. To proceed click **Install**.

11. When all the files are copied, the installation wizard displays the finish page. Click **Finish** to close the installation wizard and complete the installation.

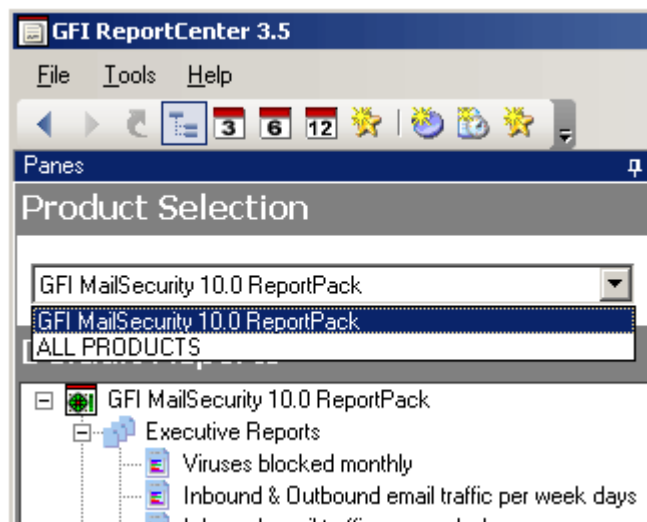
Launching GFI MailSecurity 10.0 ReportPack for GFI ReportCenter

Following the installation, you can launch the GFI MailSecurity 10.0 ReportPack for GFI ReportCenter from **Start ▶ Programs ▶ GFI ReportCenter ▶ GFI MailSecurity ReportPack**.

NOTE: GFI ReportCenter will run with limited functionality upon expiry of the evaluation period. This will also occur if the license key you entered is not a valid GFI ReportCenter license key.

Selecting a product

When more than one GFI product ReportPack is installed on the same machine, you can select the GFI product ReportPack you want to use from the **Product Selection** list.



Screenshot 116 – Product Selection list

For example, to run the reports provided in the GFI MailSecurity 10.0 ReportPack, click on the **Product Selection** list and select the GFI MailSecurity 10.0 ReportPack entry.

NOTE: Select the 'ALL PRODUCTS' option to display and navigate all the ReportPacks that are currently installed in GFI ReportCenter.

GFI MailSecurity ReportPack - Default reports

Introduction

After installing the GFI MailSecurity 10.0 ReportPack, a number of pre-configured reports can immediately be generated on the data stored in the reporting database backend of GFI MailSecurity. These default reports are organized into two categories:

Executive Reports: The executive reports group consists of eight reports that provide concise statistics and information on how GFI MailSecurity is performing. These reports are useful for people in managerial and executive positions to get a quick glance at how effective GFI MailSecurity is in protecting their network and IT infrastructure from security threats delivered through email.

The following is the complete list of executive reports:

- Viruses blocked monthly
- Inbound and outbound email traffic per week days
- Inbound email traffic per week days
- Outbound email traffic per week days
- Monthly email traffic
- Processed and blocked emails per month
- Processed emails per month
- Blocked emails per month

Administrative Reports: The administrative reports group consists of six reports that provide detailed statistics and information on how GFI MailSecurity is performing. These reports are useful for the people that administer the mail server, for example, the network administrator.

The following is the complete list of administrative reports:

- Processed and blocked emails per four hours
- Processed emails per four hours
- Blocked emails per four hours
- Daily processed and blocked emails

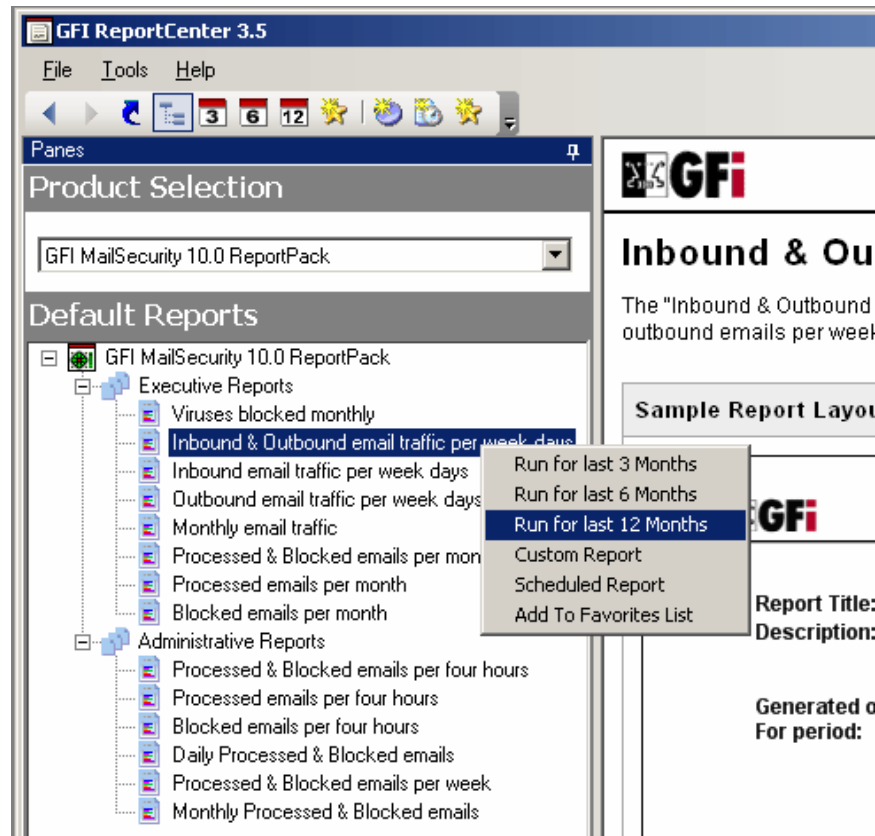
- Processed and blocked emails per week
- Monthly processed and blocked emails

GFI MailSecurity default reports are accessed by clicking on the **Default Reports** panel button.

Generating a default report

To generate a default report:

1. Click on the **Default Reports** panel button to bring up the list of default reports available.

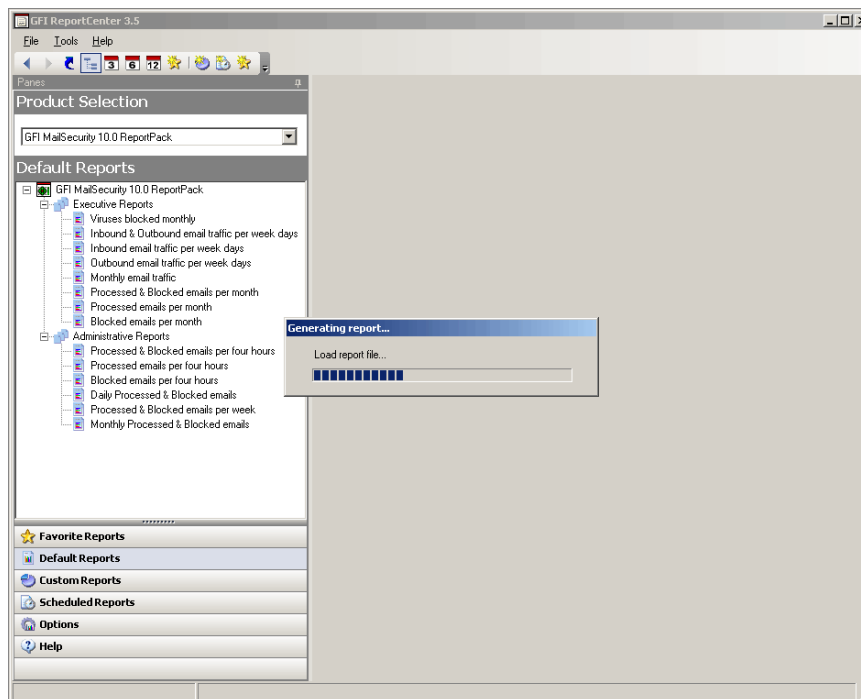


Screenshot 117 – Generating a default report

2. Right-click on the report you want to generate and click on one of the **Run for last** options.

Example: Generating a “Monthly email traffic” report based on the last 12 months data.

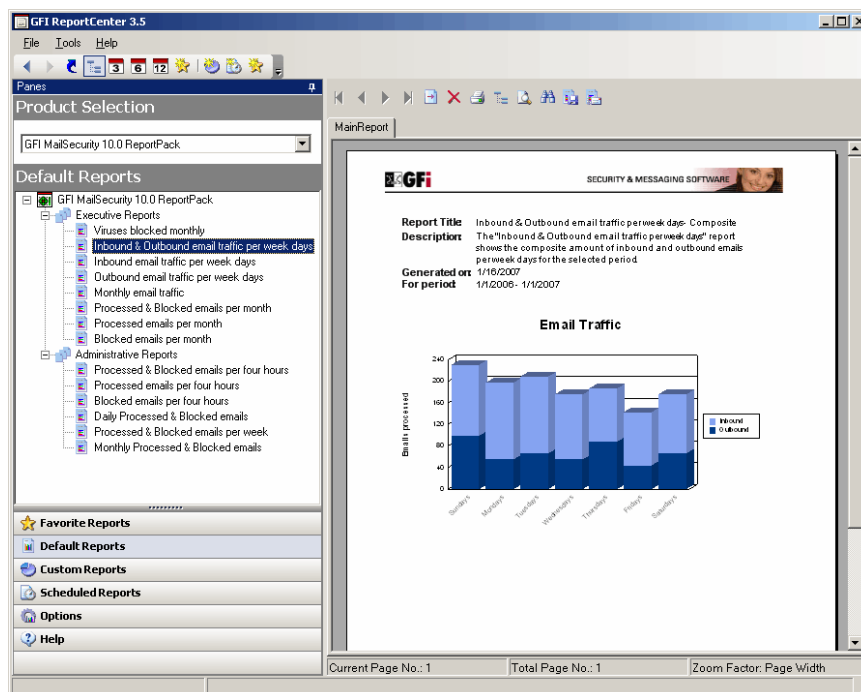
1. Click on the **Default Reports** panel button to bring up the list of available reports.
2. Expand the **Executive Reports** node and right-click on the **Monthly email traffic** report.
3. Click **Run for last 12 Months**.



Screenshot 118 - Report generation progress

Viewing the generated report







GFI ReportCenter displays the generated reports in the report-viewing pane, on the right hand side of the screen.





Screenshot 119 – Viewing a generated report

Use the toolbar at the top of the report-viewing pane to access common report related functions:

Report browsing options

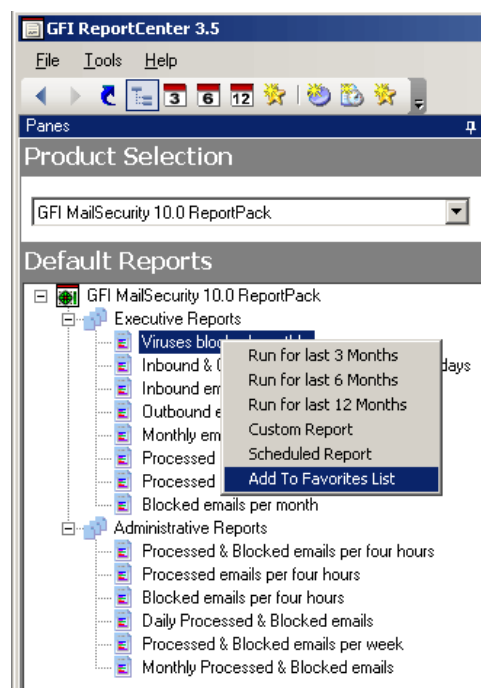
-  Browse the generated report page by page.
-  Zoom in/Zoom out.
-  Search the report for particular text or characters.
-  Go directly to a specific page.
-  Breakdown the report into a group tree (e.g. by date/time).
-  Print the report.

Report storage and distribution options

-  Export the report to a specific file format and save on a disk.
-  Distribute the generated report by email.

NOTE: For information on how to configure report storage and distribution options refer to the 'Configuring Advanced Settings' section in this manual.

Adding default reports to the list of favorite reports



Screenshot 120 – Add default report to favorites list

You can group and access frequently used reports through the **Favorite Reports** panel button. To add a default report to the list of favorite reports:

1. Click on the **Default Reports** panel button to bring up the list of available reports.
2. Right-click on the default report that you want to add to the favorites list and then click **Add to Favorites List**.

GFI MailSecurity ReportPack - Custom reports

Introduction

With GFI ReportCenter, you can create custom reports that fit specific date ranges based on the default report templates included in the GFI MailSecurity 10.0 ReportPack.

Creating a new custom report

To create a custom report:

1. Click on the **Default Reports** panel button to bring up the list of default reports available.
2. Right-click on the default report you want to base the custom report on, and then click **Custom Report** to display the **Custom Report Wizard**.



Screenshot 121 - Custom Report Wizard

3. Click **Next** to continue.
4. In the **Name and Description** page, provide a descriptive report name and description in the **Report Name** and **Report Description** boxes, and then click **Next** to continue.

Custom Report Wizard

Name and Description

Specify the name and description for this custom report

The name and description of a custom report will be used to uniquely identify the report through the set of custom reports. The custom report name must be unique.

Report name:
Inbound & Outbound email traffic per week days - 4th Quarter 2006

Report description:
The "Inbound & Outbound email traffic per week days" report shows the composite amount of inbound and outbound emails per week day for the selected period.

< Back Next > Cancel

Screenshot 122 - Report name and description for a custom report

5. In the **Date Filters** page, you need to specify what period of data you want to include in the custom report. You can either specify a fixed date range, so that the report always includes the same data, or else you can specify a variable date range, for example, for the last 6 months. When you select a variable date range, the data included in the custom report will vary depending on when the report is generated. Click **Next** to continue.

Custom Report Wizard

Date Filters

Specify the data range that should be applied to the report

☒ Fixed Date Range

Start Date: Sunday, October 01, 2006

End Date: Sunday, December 31, 2006

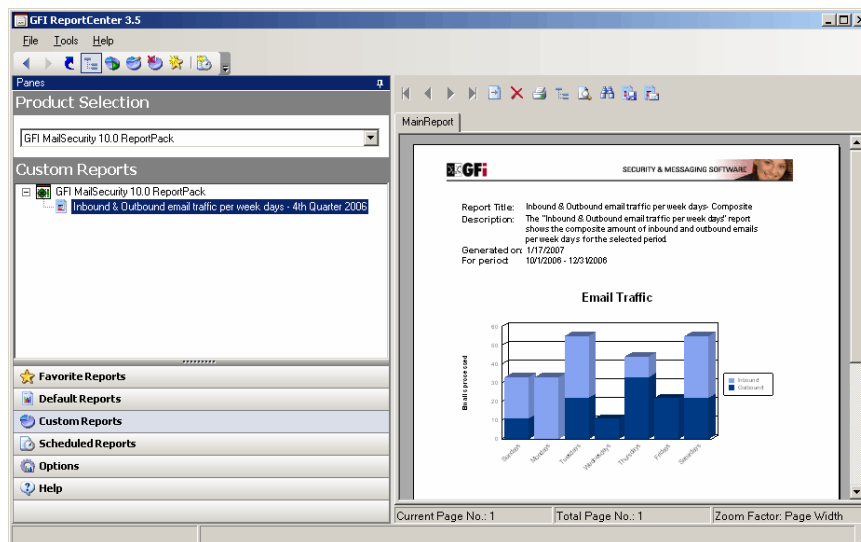
☐ Variable Range

Range Size: Choose Range Size

< Back Next > Cancel

Screenshot 123 - Selecting the date range

6. In the **Custom Report Wizard** finish page, click **Finish** to complete the wizard. GFI ReportCenter will display the **Custom Reports** panel, where the custom report you just created is listed.

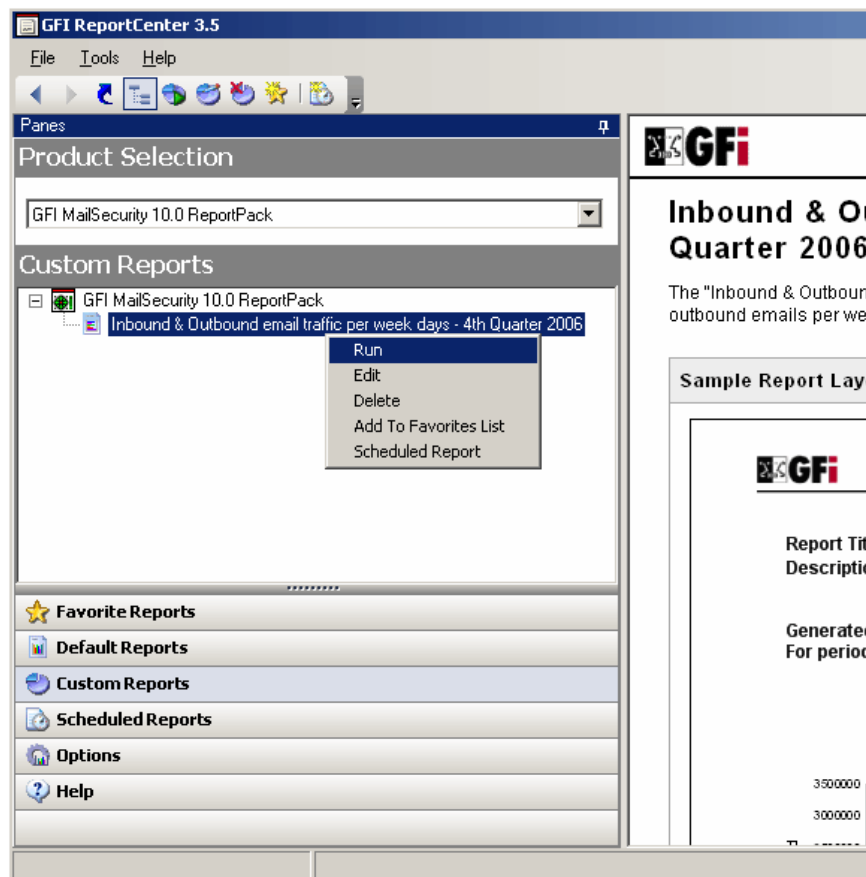


Screenshot 124 - GFI ReportCenter listing the new custom report

Generate a custom report

To generate a custom report:

1. Click on the **Custom Reports** panel button to bring up the list of custom reports available.
2. Right-click on the custom report you want to generate and then click **Run**.



Screenshot 125 - Run a custom report

Editing a custom report

To edit the configuration settings of a custom report:

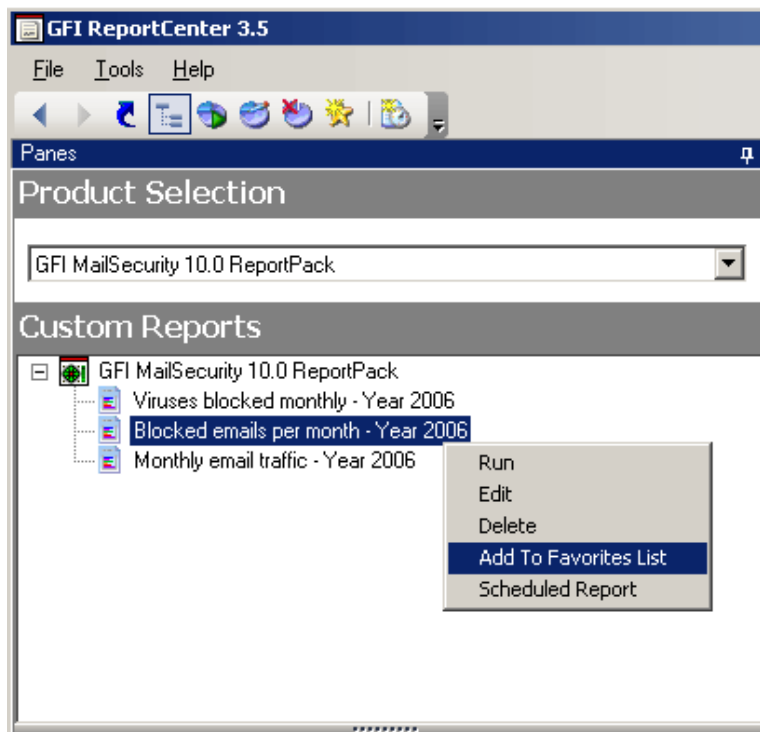
1. Click on the **Custom Reports** panel button to bring up the list of custom reports available.
2. Right-click on the custom report you want to modify and then click **Edit**. This will bring up the **Custom Report Wizard** through which you can make the required changes. For more information on how to use the **Custom Report Wizard**, refer to the 'Creating a new custom report' section earlier in this chapter.

Deleting a custom report

To delete a custom report:

1. Click on the **Custom Reports** panel button to bring up the list of custom reports available.
2. Right-click on the custom report you want to permanently remove from the list and then click **Delete**.
3. In the **Confirm** dialog box, click **Yes**.

Adding custom reports to the list of favorite reports



Screenshot 126 – Add custom report to favorites list

You can group and access frequently used reports through the **Favorite Reports** panel button. To add a custom report to the list of favorite reports:

1. Click on the **Custom Reports** panel button to bring up the list of custom reports.
2. Right-click on the custom report that you want to add to the favorites list and then click **Add to Favorites List**.

GFI MailSecurity ReportPack - Scheduling reports

Introduction

With GFI ReportCenter, you can schedule reports. You can either schedule a report to be generated once on a particular date or else to be generated periodically starting from a particular date.

With scheduling, you can thus automate the generation of reports as well as schedule the generation of reports in off peak hours, such as after office working hours, so that you make the best use of system resources.

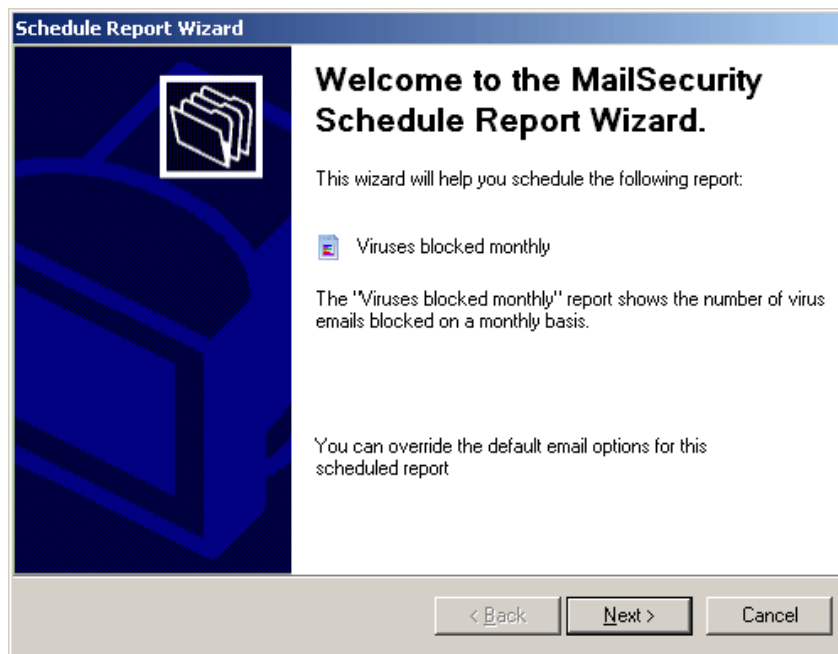
Furthermore, you can also configure GFI ReportCenter to distribute scheduled reports by email automatically. For every scheduled report, you can configure custom emailing parameters including the list of report recipients and the file format, for example, Adobe Acrobat (PDF), in which the report will be attached to the email.

Both default and custom reports can be scheduled for automatic generation.

Scheduling a report

To schedule a report, follow these steps:

1. Click on the **Default Reports** or **Custom Reports** panel button.
2. Right-click on the report you want to schedule and then click **Scheduled report** to display the **Schedule Report Wizard**.



Screenshot 127 - Schedule Report Wizard

3. Click **Next** to continue.

Screenshot 128 - Report name and description for a scheduled report

4. In the **Name and Description** page, provide a descriptive report name and description in the **Report Name** and **Report Description** boxes, and then click **Next** to continue.

Schedule Report Wizard

Time Schedule

Specify the time schedule to be used to automatically generate the report

Scheduled reports can be generated either once using a specific date and time or else re-generated using a time frame, starting from a specific time.

☐ Generate this report (once) on the following day/time:

Date/Time: 1/17/2007 12:01:02 PM

☒ Generate this report every:

Interval: 30 Days

Start date/time: 2/ 1/2007 12:00:00 AM

< Back Next > Cancel

Screenshot 129 - Scheduled report time schedule

5. In the **Time Schedule** page, select whether you want to generate the report once or periodically.

If you want to generate once on a particular date, click **Generate this report (once) on the following day/time**, then select the date and time from the calendar.

If you want to generate this report periodically starting from a particular date, click **Generate this report every**. Specify an interval amount, and then select a value from the **Interval** list. From the **Start date/time** calendar, select on which day you want to start generating this scheduled report.

Click **Next** to continue to the **Advanced Settings** page, where you can configure report distribution and storage options.

Schedule Report Wizard

Advanced Settings

Customize report distribution and storage options.

You can send the generated report by email to a target recipient list or save the generated report in a folder on your file system. Click on the Settings button of the relevant section in the dialog to further configure report sending/saving options.

☒ Export to file

Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.

Settings

☒ Send by mail

Click on the Settings button to customize and configure the email settings which will be used for report distribution.

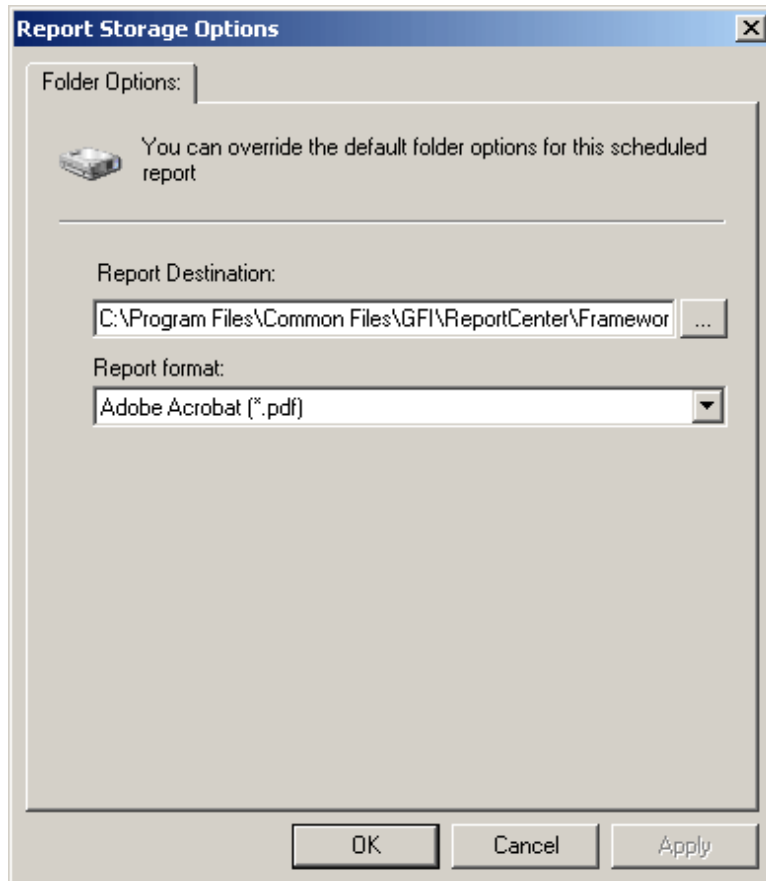
Settings

< Back Next > Cancel

Screenshot 130 - Scheduled report storage and distribution options

6. If you want to save the generated scheduled report on disk, select the **Export to file** check box. The report will be saved in the format and to the location on disk specified in the **Default Scheduling Options** dialog box. For further information, refer to the 'Configuring default scheduling options' section further on in the manual.

If you want to specify custom export to file settings for this scheduled report, click **Settings** under the **Export to file** group, to display the **Report Storage Options** dialog box. In the **Report Destination** box, specify the location on disk where you want this scheduled report to be saved and then select an export format from the **Report format** list. Click **OK** to close the **Report Storage Options** dialog box.



Screenshot 131 - Custom scheduled report storage options

7. If you want to send the generated scheduled report by email, select the **Send by mail** check box. The report will be sent to the recipients using the SMTP server specified in the **Default Scheduling Options** dialog box. For further information, refer to the 'Configuring default scheduling options' section further on in the manual.

If you want to specify custom send by email settings for this scheduled report, click **Settings** under the **Send by mail** group, to display the **Email Alerts Options** dialog box.

Specify the following parameters:

- **To/CC:** Specify the email address (es) where you want to send the scheduled report.
- **From:** Specify the email account that will be used to send the report.

- **Server:** Specify the machine name or IP address of your SMTP (outbound) email server. If the specified server requires authentication, select the **SMTP Server requires login** check box and specify the logon credentials in the **User name** and **Password** boxes.
- **Report format:** Reports are sent via email as attachments. Select the file format in which you want to send the scheduled report from the list.

Click **OK** to close the **Email Alerts Options** dialog box.

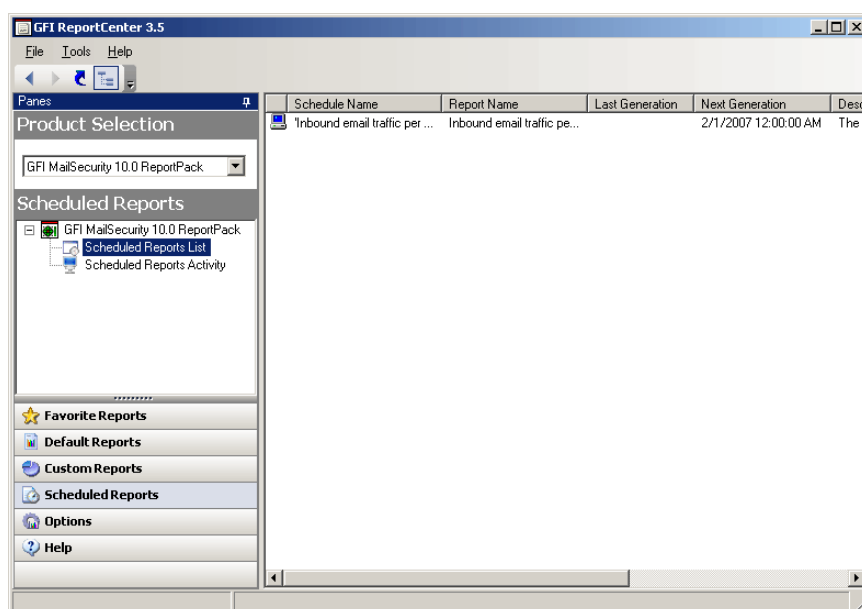
Screenshot 132 - Custom scheduled email distribution options

8. Click **Next** to continue.

9. If you are scheduling a custom report, go to point 10 below. If you are scheduling a default report, the **Date Filters** page is displayed so that you can specify a date range for the report. In the **Date Filters** page, you need to specify what period of data you want to include in the scheduled report. You can either specify a fixed date range, so that the report always includes the same data, or else you can specify a variable date range, for example, for the last 6 months. When you select a variable date range, the data included in the scheduled report will vary depending on when the report is generated. Click **Next** to continue.

10. In the **Schedule Report Wizard** finish page, click **Finish** to complete the wizard.

Viewing the list of scheduled reports



Screenshot 133 - List of scheduled reports

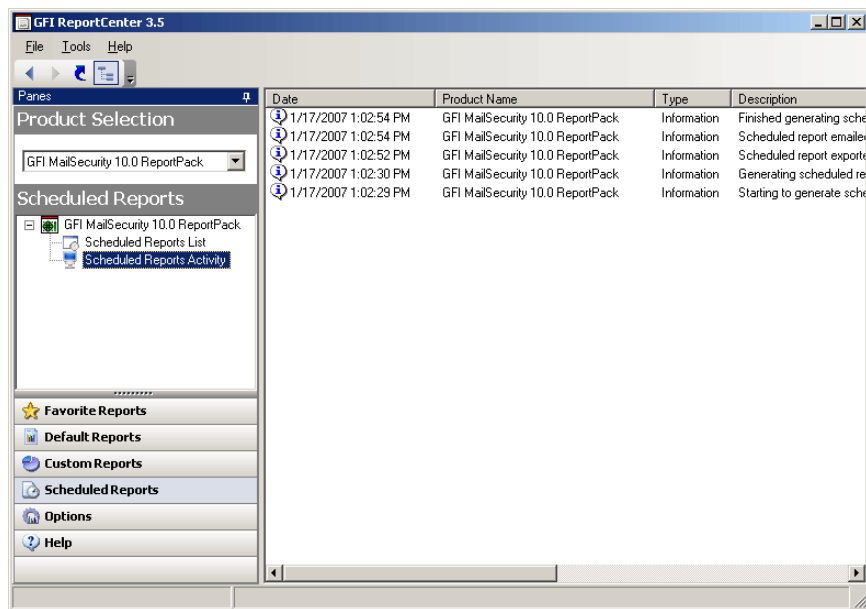
To view the list of scheduled reports, click on the **Scheduled Reports** panel button and then click on the **Scheduled Reports List** node. The following details are displayed:

- **Schedule Name:** The custom name that was specified during the creation of the scheduled report.
- **Report Name:** The name of the default or custom report scheduled.
- **Last Generation:** Shows when the last report was generated.
- **Next Generation:** Shows when the next report will be generated.
- **Description:** The description you specified when creating the scheduled report.

Viewing the scheduled reports activity




GFI ReportCenter also includes a schedule activity monitor through which you can view events related to the generation of scheduled reports.

To open the schedule activity monitor, click on the **Scheduled Reports** panel button and then click the **Scheduled Reports Activity** node. The activity information is displayed in the right pane of the GFI ReportCenter management console.



Screenshot 134 - Schedule activity monitor

The activity monitor displays the following events:

-  **Information:** The scheduled report was successfully generated.
-  **Warning:** The scheduled report was not generated since the product license is invalid or has expired.
-  **Error:** The scheduled report was not generated due to some error. Typical errors include:

- Errors when attempting to save the generated report to a specific location on disk, for example, out of disk space.
- Errors when attempting to send the generated report by email, for example, the SMTP server configured in the GFI ReportCenter settings is not reachable.

The activity monitor records and displays the following information:

- **Date:** The date and time when the scheduled report was executed.
- **Product name:** The name of the GFI product ReportPack to which the report belongs.
- **Type:** The event classification - error, information, or warning.
- **Description:** Information related to the state of a scheduled report that has been executed. The format and contents of the activity description vary, depending on the event type.

NOTE: The description is often the most useful piece of information, indicating what happened during the execution of a scheduled report or the significance of the event.

Enable/disable a scheduled report

Scheduled reports can be enabled or disabled as required.

To disable a scheduled report, follow these steps:

1. Click on the **Scheduled Reports** panel button and then click on the **Scheduled Reports List** node.

2. Right-click on the scheduled report you want to disable and then click **Disable**.

The status of scheduled reports is indicated by an icon to the left of each scheduled report as follows:



- Indicates that the scheduled report is disabled.



- Indicates that the scheduled report is enabled.

To enable a scheduled report, follow these steps:

1. Click on the **Scheduled Reports** panel button and then click on the **Scheduled Reports List** node.
2. Right-click on the scheduled report you want to enable and then click **Enable**.

Editing a scheduled report

To make changes to the configuration settings of a scheduled report:

1. Click on the **Scheduled Reports** panel button and then click on the **Scheduled Reports List** node.
2. Right-click on the scheduled report you want to re-configure and then click **Properties**, to load the **Schedule Reports Wizard**.
3. Use the wizard to modify the scheduled report settings as required. For information on how to configure the parameters of a scheduled report, refer to the 'Scheduling a report' section earlier in this chapter.

Deleting a scheduled report

To delete a scheduled report:

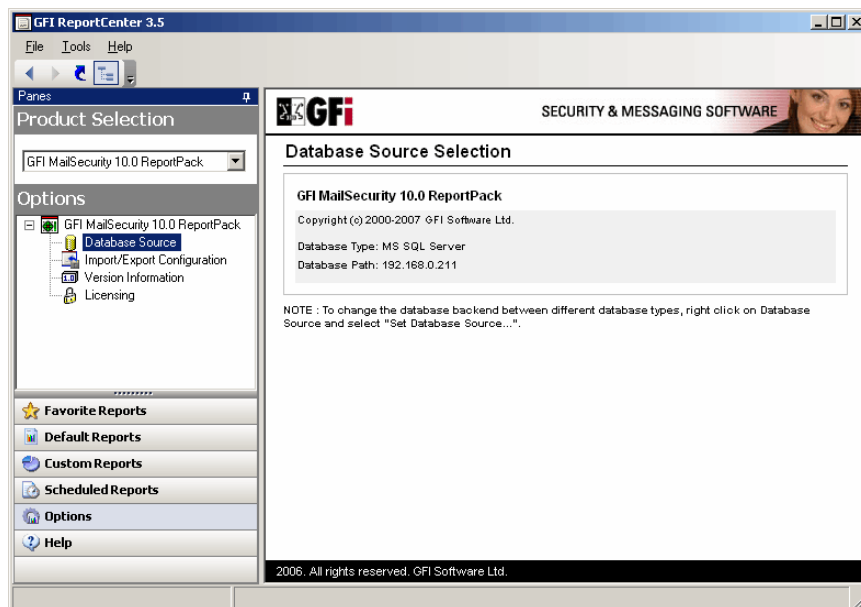
1. Click on the **Scheduled Reports** panel button and then click on the **Scheduled Reports List** node.
2. Right-click on the scheduled report you want to delete and then click **Delete**.
3. In the **Confirm** dialog box, click **Yes**.

GFI MailSecurity ReportPack - Configuring default options

Introduction

While installing the GFI MailSecurity 10.0 ReportPack, you configured some default settings that are used by the GFI ReportCenter when distributing reports by email and storing reports to disk, as well as on which GFI MailSecurity reporting database you want to base the reports. If the need arises, you can re-configure these settings from the GFI ReportCenter management console as shown in the following sections.

Which GFI MailSecurity reporting database is being used?



Screenshot 135 – GFI MailSecurity reporting database

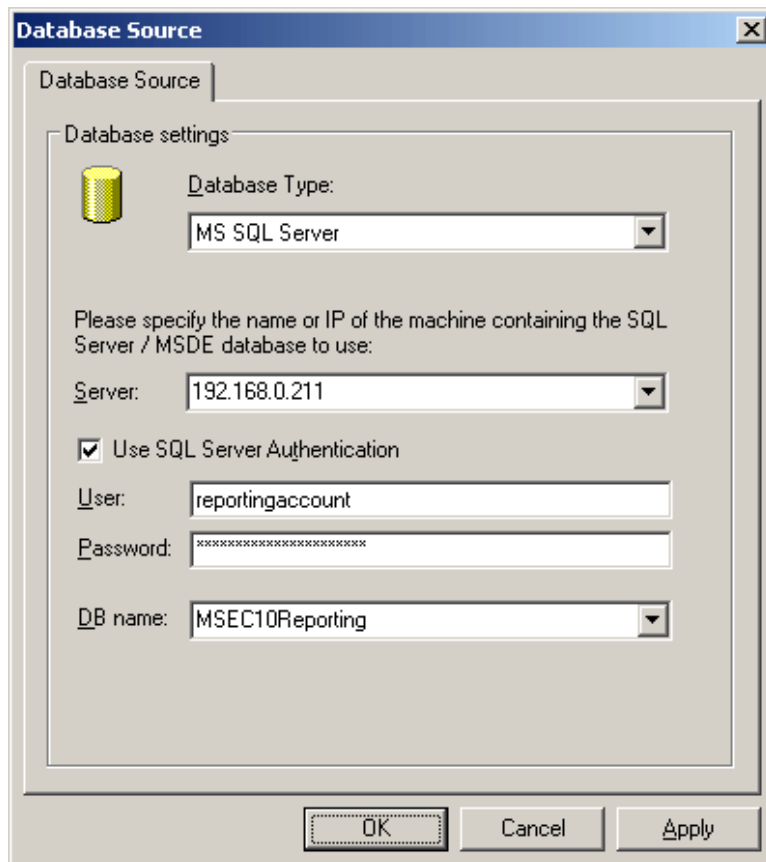
To check which GFI MailSecurity reporting database source is currently being used by the GFI ReportCenter to generate reports, follow these steps:

1. Click on the **Options** panel button.
2. Click on the **Database Source** node to view the current GFI MailSecurity reporting database details in the right-pane.

Configuring the GFI MailSecurity reporting database source

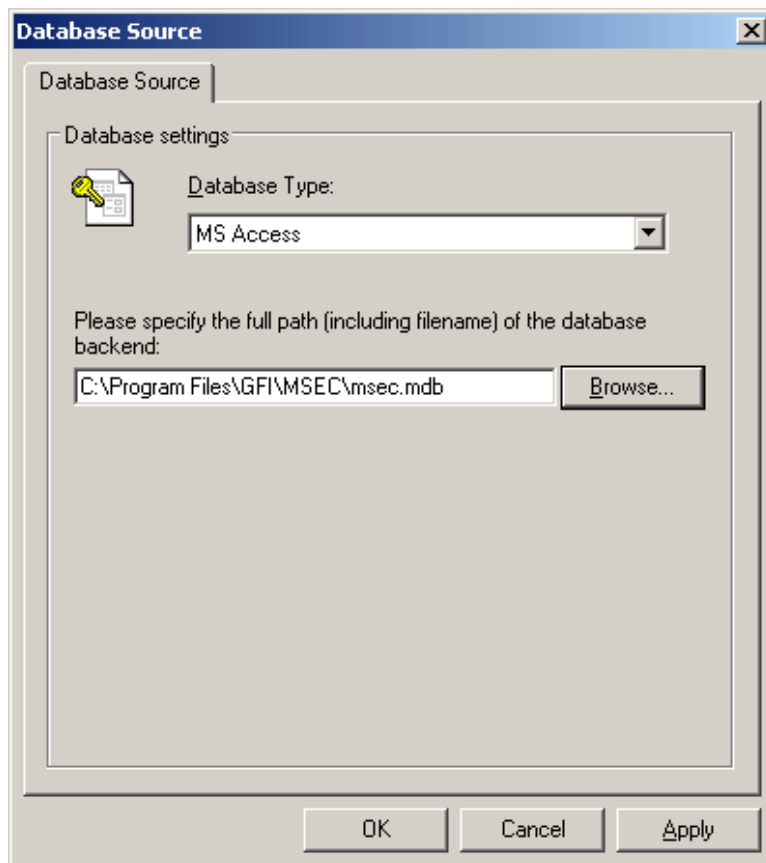
To change the GFI MailSecurity reporting database source, follow these steps:

1. Click on the **Options** panel button.
2. Right-click on the **Database Source** node and then click **Set Database Source**.



Screenshot 136 - Microsoft SQL Server reporting database

3. Select the reporting database type, from the **Database Type** list. If you selected Microsoft Access, go to step 5. If you selected Microsoft SQL Server, go to step 4.
4. Specify the machine name or IP address of the server hosting Microsoft SQL Server in the **Server** box. If you use Windows Authentication, clear the **Use SQL Server Authentication** check box. If you use Microsoft SQL Server authentication, select the **Use SQL Server Authentication** check box and specify a user name and password in the **User** box and **Password** box respectively. From the **DB Name** list, select the GFI MailSecurity reporting database.
5. If you selected Microsoft Access, specify the full path to the Microsoft Access database, in which GFI MailSecurity is logging reporting data, in the space provided. You can do this either by typing the path in the box or else click **Browse** and then select the Microsoft Access file visually from the dialog box.



Screenshot 137 – Microsoft Access reporting database

6. Click **OK** to save the new settings and close the **Database Source** dialog box.

Configuring default scheduling options

To configure the default settings the scheduled reports use when distributing reports by email or saving to disk, follow these steps:

1. On the **Tools** menu, click **Default Scheduling Options**.
2. Configure the default email options as outlined in point 7 of the 'Scheduling a report' section earlier in the manual.
3. Configure the default folder options as outlined in point 6 of the 'Scheduling a report' section earlier in the manual.
4. Click **OK** to save the new settings and close the **Default Scheduling Settings** dialog box.

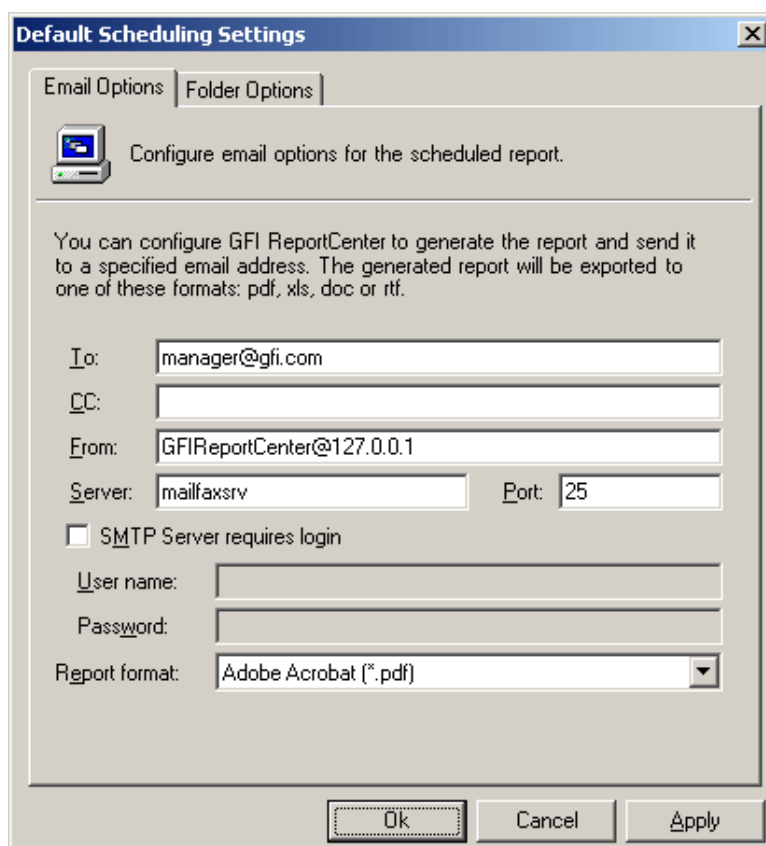
Reports can be exported to disk or attached to an email in any one of the following file formats:

Adobe Acrobat (.PDF) - Use this format to allow distribution of a report on different systems such as Macintosh and Linux while preserving the layout.

Microsoft Excel (.XLS) - Use this format if you want to process the report further in Microsoft Excel.

Microsoft Word (.DOC) - Use this format if you want to access this report using Microsoft Word.

Rich Text Format (.RTF) - Use this format to save the report in a format that consumes less disk space and which allows accessibility through different word processors in different operating systems.



The screenshot shows a Windows-style dialog box titled "Default Scheduling Settings". It has two tabs: "Email Options" (selected) and "Folder Options". Below the tabs is a small icon of a computer monitor and the text "Configure email options for the scheduled report." Below this is a paragraph: "You can configure GFI ReportCenter to generate the report and send it to a specified email address. The generated report will be exported to one of these formats: pdf, xls, doc or rtf." The form contains several input fields: "To:" with the value "manager@gfi.com", "CC:" (empty), "From:" with the value "GFIReportCenter@127.0.0.1", "Server:" with the value "mailfaxsrv", and "Port:" with the value "25". There is a checkbox labeled "SMTP Server requires login" which is currently unchecked. Below this are fields for "User name:" and "Password:" (both empty). At the bottom is a "Report format:" dropdown menu currently set to "Adobe Acrobat (*.pdf)". At the very bottom are three buttons: "Ok", "Cancel", and "Apply".

Screenshot 138 - Default Scheduling Settings

GFI MailSecurity ReportPack - General options

Entering your license key after installation

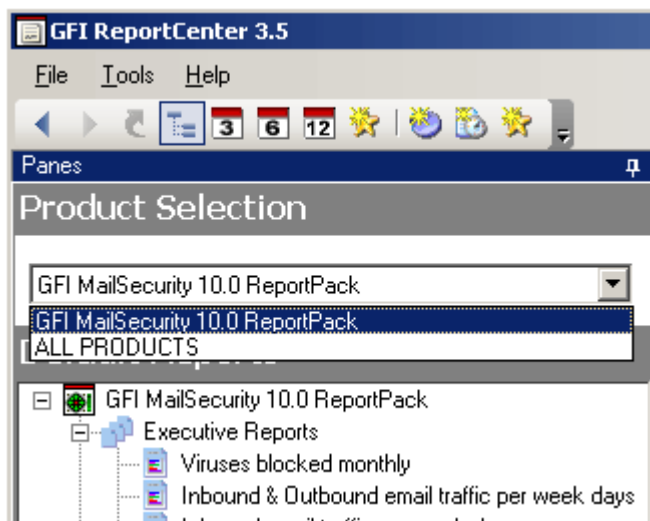
If you purchased a license key for the GFI MailSecurity 10.0 ReportPack, enter your License key using the **Options ▶ Licensing** node (no re-installation/re-configuration required)

NOTE 1: You must purchase a different license key for every GFI product ReportPack to be installed and accessed through the GFI ReportCenter framework.

For example, to install both the GFI FAXmaker 12.0 ReportPack and the GFI MailSecurity 10.0 ReportPack, you must purchase two separate license keys, one for each product ReportPack.

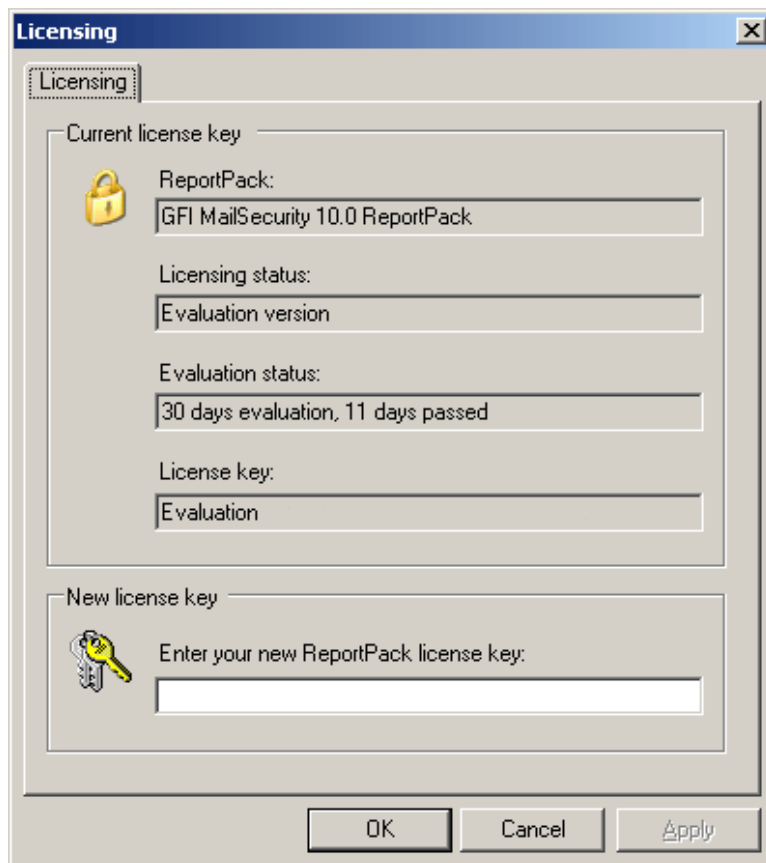
NOTE 2: Entering the License Key should not be confused with the process of registering your company details on our website. This is important since it allows us to give you support and notify you of important product news. You may register and obtain your GFI customer account from <http://www.gfi.com/pages/regfrm.htm>.

To input your GFI MailSecurity 10.0 ReportPack license key:



Screenshot 139 – Product Selection list

1. Select GFI MailSecurity 10.0 ReportPack, from the **Product Selection** list.
2. Click on the **Options** panel button.
3. Right-click on the **Licensing** node and then click **Set Licensing....**



Screenshot 140 - Licensing dialog

4. Type in the GFI MailSecurity 10.0 ReportPack license key.
5. Click **OK**.

Viewing the current licensing details

To view your current licensing details, click on the **Options** panel button and select the **Licensing** node. The licensing details are displayed in the right pane of the management console.

Viewing the GFI MailSecurity 10.0 ReportPack version details

To view the version information of the GFI MailSecurity 10.0 ReportPack:

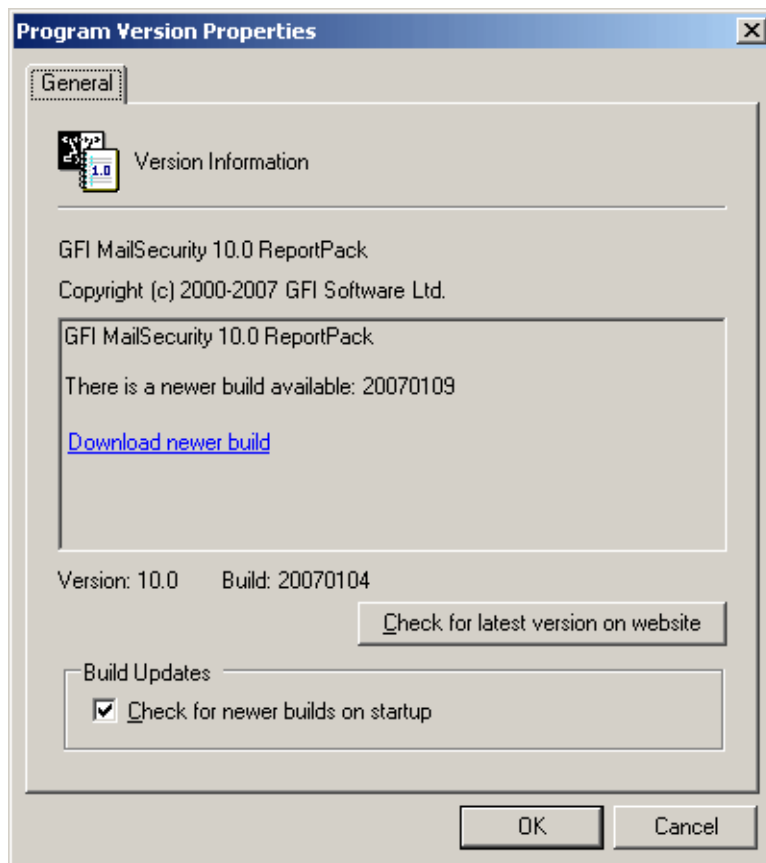
1. Select GFI MailSecurity 10.0 ReportPack from the **Product Selection** list.
2. Click on the **Options** panel button and then click on the **Version Information** node. The version details will be displayed in the right pane of the management console.

Checking the web for newer builds

Periodically GFI releases product and ReportPack updates that can be automatically downloaded from the GFI website. To check if a newer build is available for download:

1. Select the GFI MailSecurity 10.0 ReportPack from the **Product Selection** list.

2. Click on the **Options** panel button.
3. Right-click on the **Version Information** node and select **Checking for newer builds...**



Screenshot 141 - Version Properties: Checking for newer builds

GFI MailSecurity ReportPack - Exporting Settings

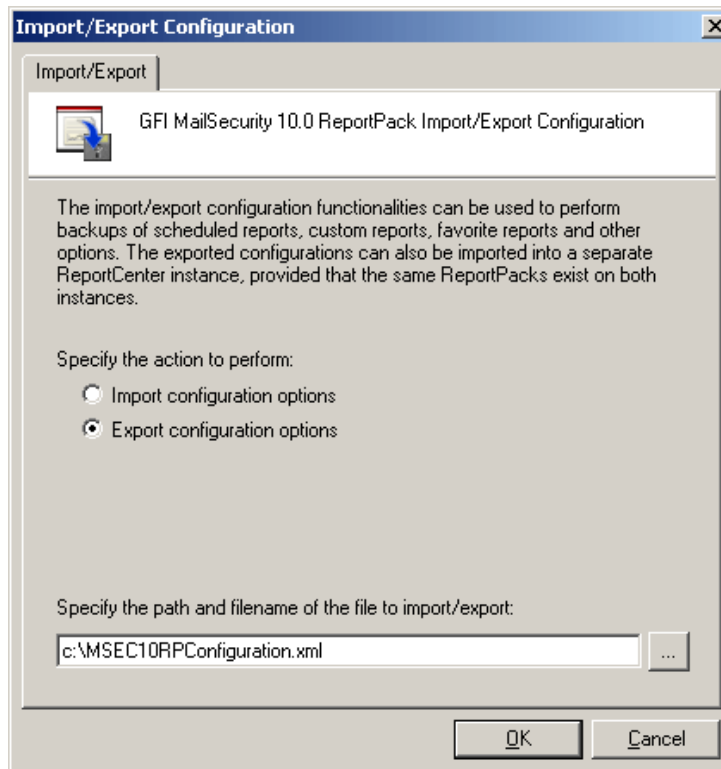
Introduction

This section will show you how to export the settings configured for the GFI MailSecurity 10.0 ReportPack into an XML file. This is useful if you need to take a backup of the favorite reports list and the configured custom and scheduled reports. Exporting settings is also useful if you need to setup an installation of GFI ReportCenter on another machine. For this scenario, you need to export the settings from the configured GFI ReportCenter installation, copy the exported XML file over to the other machine where the new installation of GFI ReportCenter is installed, and then import the settings from the XML file.

Exporting the GFI MailSecurity 10.0 ReportPack Settings

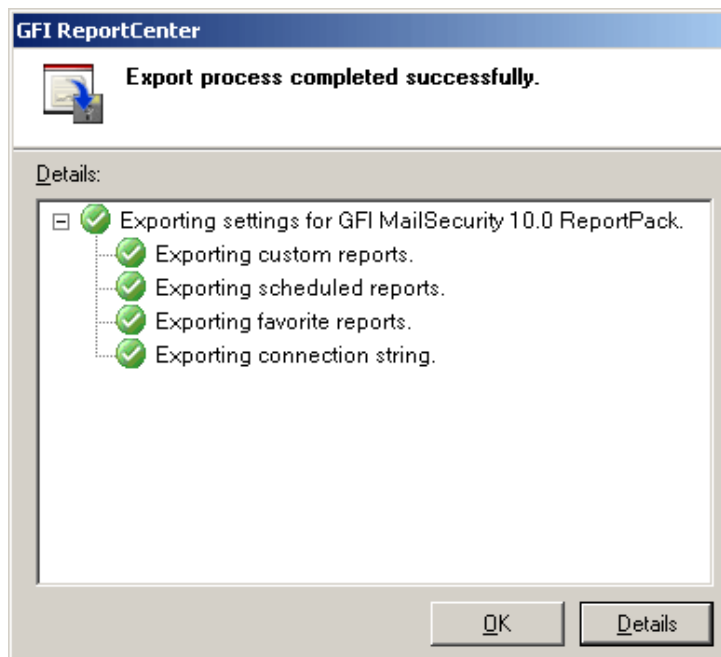
To export all the settings for the GFI MailSecurity 10.0 ReportPack, follow these steps:

1. Click on the **Options** panel button.
2. Right-click on the **Import/Export Configuration** node and then click **Import/Export Configuration**.



Screenshot 142 - Export setting dialog box

3. Click **Export configuration options**.
4. Type the full path, including filename with extension XML, in the box provided, to specify where you want the exported settings to be saved.
5. Click **OK** to start the export process.
6. When the settings are exported successfully, the following dialog box is displayed.



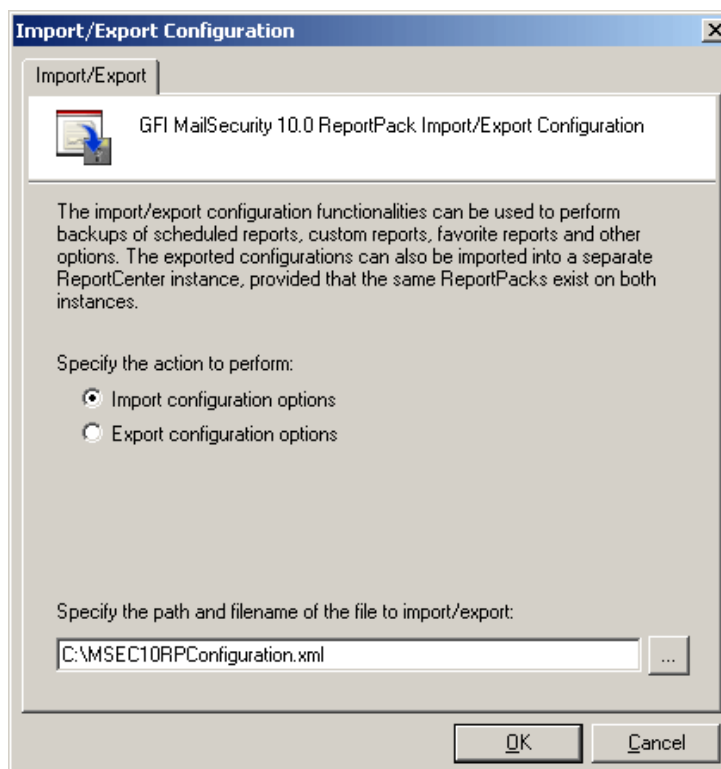
Screenshot 143 - Settings exported successfully

7. Click **OK** to close the dialog box.

Importing the GFI MailSecurity 10.0 ReportPack Settings

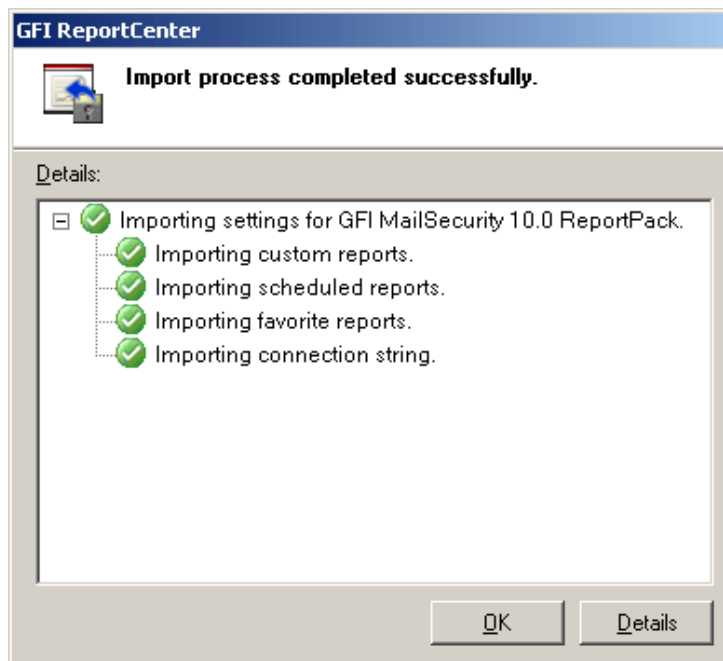
To import GFI MailSecurity 10.0 ReportPack settings, follow these steps:

1. Click on the **Options** panel button.
2. Right-click on the **Import/Export Configuration** node and then click **Import/Export Configuration**.
3. Click **Import configuration options**.
4. Type the full path, including filename with extension XML, in the box provided, to specify from which XML file you want to import the GFI MailSecurity 10.0 ReportPack settings.



Screenshot 144 - Import setting dialog box

5. Click **OK** to start the import process.
6. When the settings are imported successfully, the following dialog box is displayed.



Screenshot 145 - Settings exported successfully

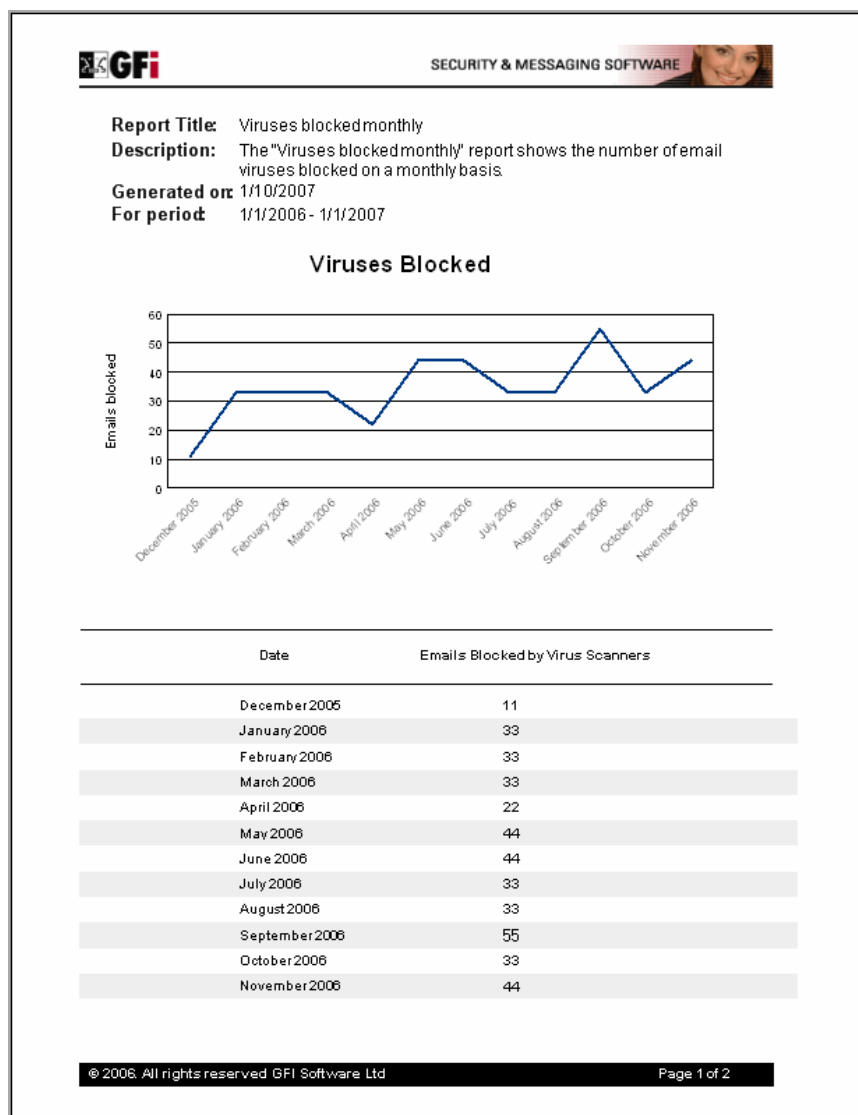
7. Click **OK** to close the dialog box.
8. For the imported settings to take effect, you need to exit GFI ReportCenter, and then start it.

GFI MailSecurity ReportPack - Default Reports List

Executive Reports

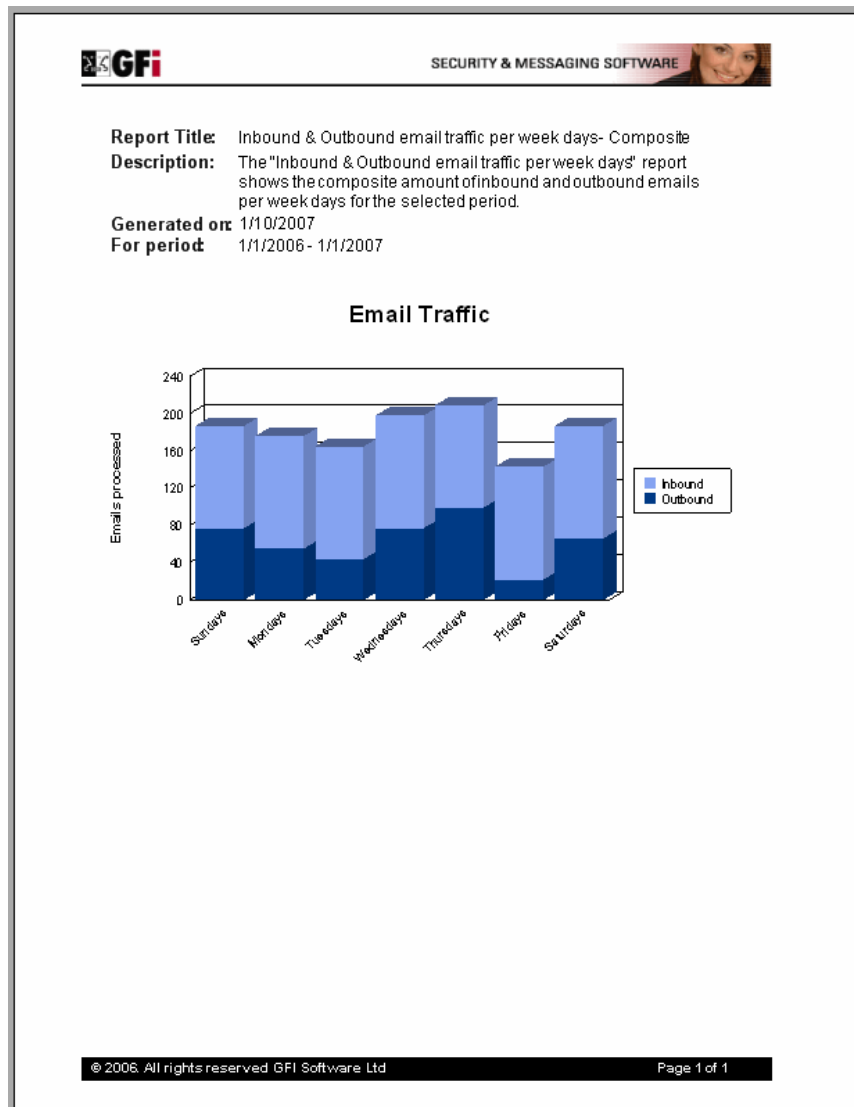
Viruses Blocked Monthly

This report shows you how many virus-infected emails GFI MailSecurity blocked per month in a table. The graph included in the report will help you visualize information such as virus outbreak trends.



Inbound and outbound email traffic per week days

This report combines the amount of emails sent and received during a particular period into a single week to present a bar graph showing inbound and outbound traffic for each day of the week. Since the amount of emails sent or received on each day of the week is stacked on the same bar, you can visually determine the ratio of emails sent versus received on the mail server. Through this report, you can conclude on which days of the week the mail server is most busy. This could help you determine the right day of the week to perform maintenance on the mail server.



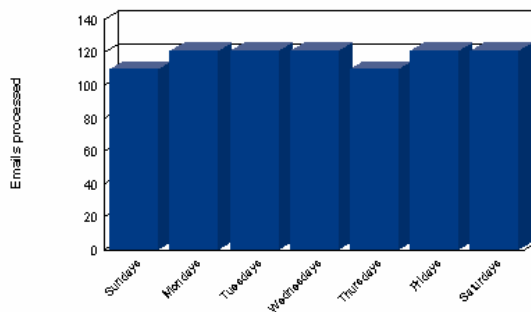
Inbound email traffic per week days

This report combines the amount of emails received during a particular period into a single week to present a bar graph showing inbound traffic for each day of the week. Through this report, you can determine on which days of the week the mail server receives the most emails.



Report Title: Inbound email traffic per week days- Composite
Description: The "Inbound email traffic per week days" report shows the composite amount of inbound emails per week days for the selected period
Generated on: 1/10/2007
For period: 1/1/2006 - 1/1/2007

Email Traffic



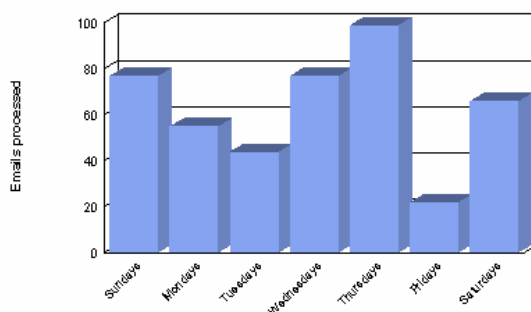
Outbound email traffic per week days

This report combines the amount of emails sent during a particular period into a single week to present a bar graph showing outbound traffic for each day of the week. Through this report, you can determine on which days of the week your organization sends the most emails.



Report Title: Outbound email traffic per week days- Composite
Description: The "Outbound email traffic per week days" report shows the composite amount of outbound emails per week days for the selected period
Generated on: 1/10/2007
For period: 1/1/2006 - 1/1/2007

Email Traffic



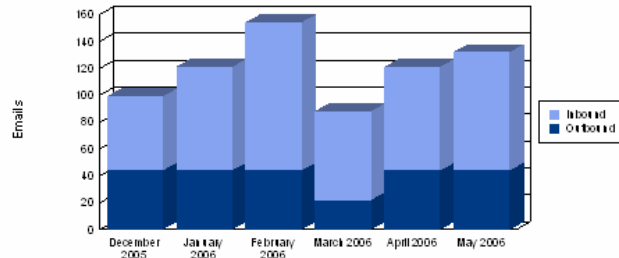
Monthly email traffic

This report shows you how many emails were received and sent per month in a table. The report further includes a stacked bar graph of the data present in the table to help you visualize traffic trends over the period selected for the report. Since the amount of emails sent or received per month is stacked on the same bar, you can visually determine the ratio of emails sent versus received on the mail server. This report can help you decide whether you need to upgrade the mail server hardware to handle the increasing mail flow, for example.



Report Title: Monthly email traffic
Description: The "Monthly email traffic" report shows the amount of inbound and outbound emails per month for the selected period.
Generated on: 1/10/2007
For period: 12/1/2005 - 5/31/2006

Email Traffic



Date	Inbound	Outbound
December 2005	55	44
January 2006	77	44
February 2006	110	44
March 2006	66	22
April 2006	77	44
May 2006	88	44
	473	242

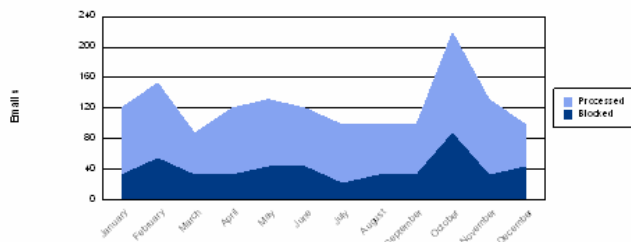
Processed and blocked emails per month

This report combines data from the period you select into the twelve months to show you how many emails were processed, blocked due to a security threat and what percentage of the processed emails was blocked email for each month of the year. The same data is also presented as an area graph. Apart from getting a picture of how email traffic patterns vary from month to month, you can also spot interesting trends regarding the amount of security threats received. Furthermore, this report provides a total sum of emails processed and blocked for the period you select.



Report Title: Processed & Blocked emails per month- Composite
Description: The "Processed & Blocked emails per month" report shows the composite amount of blocked emails against processed emails per month for the selected period
Generated on: 1/10/2007
For period: 1/10/2005 - 1/10/2007

Blocked emails



Month	Processed Emails	Blocked Emails	Percentage of Blocked Emails
January	121	33	27.27%
February	154	55	35.71%
March	88	33	37.50%
April	121	33	27.27%
May	132	44	33.33%
June	121	44	36.36%
July	99	22	22.22%
August	99	33	33.33%
September	99	33	33.33%
October	221	88	39.82%
November	132	33	25.00%
December	99	44	44.44%
	<u>1,486</u>	<u>495</u>	<u>32.97%</u>

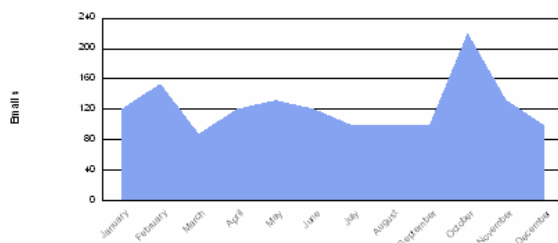
Processed emails per month

This report combines data from the period you select into the twelve months to show you how many emails were processed for each month of the year. The same data is also presented as an area graph.



Report Title: Processed emails per month- Composite
Description: The "Processed emails per month" report shows the composite amount of processed emails per month for the selected period.
Generated on: 1/10/2007
For period: 1/10/2005 - 1/10/2007

Processed Emails



Month	Processed Emails
January	121
February	154
March	88
April	121
May	132
June	121
July	99
August	99
September	99
October	221
November	132
December	99
	<u>1,486</u>

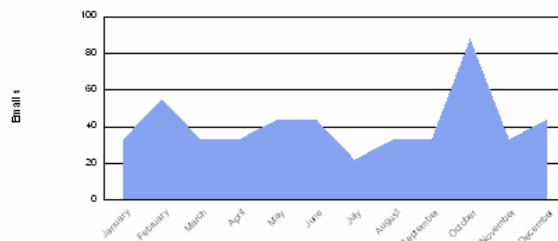
Blocked emails per month

This report combines data from the period you select into the twelve months to show you how many emails were blocked due to a security threat for each month of the year. The same data is also presented as an area graph.



Report Title: Blocked emails per month- Composite
Description: The "Blocked emails per month" report shows the composite amount of blocked emails per month for the selected period.
Generated on: 1/10/2007
For period: 1/10/2005 - 1/10/2007

Blocked emails



Month	Blocked Emails
January	33
February	55
March	33
April	33
May	44
June	44
July	22
August	33
September	33
October	88
November	33
December	44
	<u>495</u>

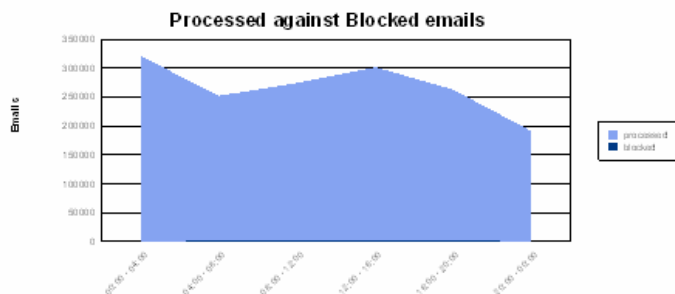
Administrative Reports

Processed and blocked emails per four hours

This report combines data from the period you select into a single day to show you how many emails were processed, blocked due to a security threat and what percentage of the processed emails was blocked email in four hour blocks starting from midnight. The same data is also presented as an area graph. Through this report, you can get a picture of how email traffic and security threat patterns vary throughout the day. Furthermore, this report provides a total sum of emails processed and blocked for the period you select.



Report Title: Processed & Blocked emails per four hours - Composite
Description: The "Processed & Blocked emails per four hours" report shows the composite amount of blocked emails against processed emails in four hour blocks for the selected period.
Generated on: 29/08/2006
For period: 22/08/2006 - 29/08/2006



Hour	Processed Emails	Blocked Emails	Percentage of Blocked Emails
00:00 - 04:00	320,867	863	0.27%
04:00 - 08:00	252,575	1,900	0.75%
08:00 - 12:00	274,844	2,665	0.97%
12:00 - 16:00	301,962	2,175	0.72%
16:00 - 20:00	263,159	2,468	0.93%
20:00 - 00:00	191,729	931	0.49%
	<u>1,604,936</u>	<u>10,992</u>	<u>0.69%</u>

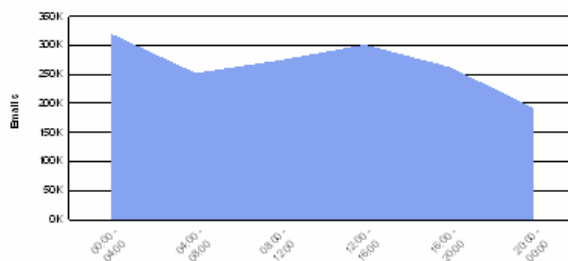
Processed emails per four hours

This report combines data from the period you select into a single day to show you how many emails were processed in four-hour blocks. The same data is also presented as an area graph.



Report Title: Processed emails per four hours - Composite
Description: The "Processed emails per four hour" report shows the composite amount of processed emails in four hour blocks for the selected period.
Generated on: 29/08/2006
For period: 22/08/2006 - 29/08/2006

Processed emails



Hour	Processed Emails
00:00 - 04:00	320,867
04:00 - 08:00	252,575
08:00 - 12:00	274,844
12:00 - 16:00	301,962
16:00 - 20:00	263,159
20:00 - 00:00	191,729
	<u>1,604,936</u>

Blocked emails per four hours

This report combines data from the period you select into a single day to show you how many emails were blocked due to a security threat in four-hour blocks. The same data is also presented as an area graph.



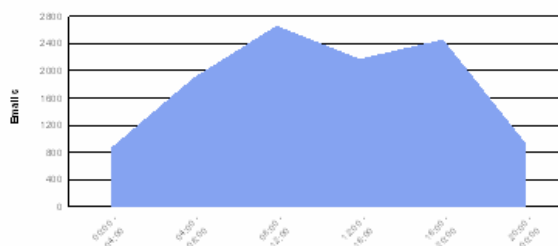
Report Title: Blocked emails per four hours - Composite

Description: The "Blocked emails per four hour" report shows the composite amount of blocked emails in four hour blocks for the selected period.

Generated on: 29/08/2006

For period: 22/08/2006 - 29/08/2006

Blocked emails



Hour	Blocked Emails
00:00 - 04:00	863
04:00 - 08:00	1,900
08:00 - 12:00	2,665
12:00 - 16:00	2,175
16:00 - 20:00	2,458
20:00 - 00:00	931
	10,992

Daily processed and blocked emails

This report displays how many emails were processed, blocked due to a security threat and what percentage of the processed emails was blocked email for each day in the period you select. Furthermore, this report provides a total sum of emails processed and blocked for the period you select.

**Report Title:** Daily blocked emails**Description:** The "Daily blocked emails" report shows the amount of blocked emails against processed emails per day for the selected period.**Generated on:** 09/08/2006**For period:** 26/07/2006 -09/08/2006

Day	Processed Emails	Blocked Emails	Percentage of Blocked Emails
26/07/2006	95,115	760	0.80%
27/07/2006	123,267	1,085	0.88%
28/07/2006	123,877	699	0.56%
29/07/2006	121,474	469	0.39%
30/07/2006	89,495	888	0.99%
31/07/2006	117,909	378	0.32%
01/08/2006	133,913	670	0.50%
02/08/2006	134,765	705	0.52%
03/08/2006	114,169	852	0.75%
04/08/2006	141,347	968	0.68%
05/08/2006	119,499	524	0.44%
06/08/2006	86,974	875	1.01%
07/08/2006	160,816	688	0.43%
08/08/2006	75,107	987	1.31%
	<u>1,637,727</u>	<u>10,548</u>	<u>0.68%</u>

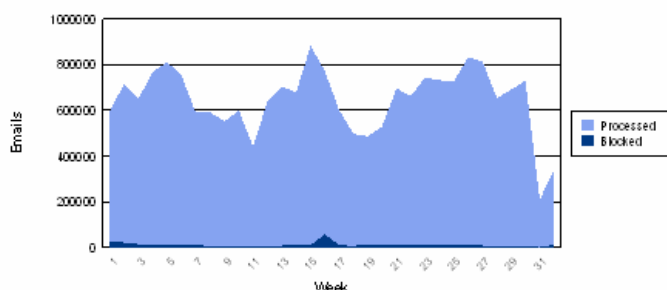
Processed and blocked emails per week

This report combines data from the period you select into a single year to show you how many emails were processed, blocked due to a security threat and what percentage of the processed emails was blocked email during each week of the year. The same data is also presented as an area graph. Apart from getting a picture of how email traffic patterns vary from week to week throughout the year, you can also spot interesting trends regarding the amount of security threats received. Furthermore, this report provides a total sum of emails processed and blocked for the period you select.



Report Title: Blocked emails per week
Description: The "Blocked emails per week" report shows the composite amount of blocked emails against processed emails per week for the selected period.
Generated on: 09/08/2006
For period: 09/08/2004 - 09/08/2006

Blocked emails



Week	Processed Emails	Blocked Emails	Percentage of Blocked Emails
1	598,011	21,935	3.67%
2	713,893	21,884	3.07%
3	650,469	14,783	2.27%
4	769,973	9,659	1.25%
5	810,995	9,472	1.17%
6	754,190	14,838	1.97%
7	588,745	9,381	1.59%
8	590,925	6,429	1.09%
9	552,037	6,515	1.18%
10	598,390	6,407	1.07%
11	439,910	6,246	1.42%
12	640,540	6,929	1.08%
13	702,867	8,322	1.18%
14	679,289	12,085	1.78%
15	882,363	10,325	1.17%
16	773,109	58,488	7.57%

Monthly processed and blocked emails

This report lists the amount of emails processed, blocked due to a security threat and what percentage of the processed emails was blocked email for each month during the period selected. Furthermore, this report provides a total sum of emails processed and blocked for the period you select.



Report Title: Monthly blocked emails

Description: The "Monthly blocked emails" report shows the amount of blocked emails against processed emails per month for the selected period.

Generated on: 09/08/2006

For period: 01/08/2004 - 01/08/2006

Month	Processed Emails	Blocked Emails	Percentage of Blocked Emails
December 2005	342,974	13,350	3.89%
January 2006	3,088,137	71,961	2.33%
February 2006	2,613,065	38,900	1.49%
March 2006	2,613,175	31,036	1.19%
April 2006	3,105,199	91,655	2.95%
May 2006	2,509,856	49,335	1.97%
June 2006	3,219,059	48,461	1.51%
July 2006	3,198,477	30,543	0.95%
	<u>20,689,942</u>	<u>375,241</u>	<u>2.03%</u>

GFI MailSecurity ReportPack - Troubleshooting

Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

- The manual – most issues can be solved by reading this manual.
- GFI Knowledge Base articles
- Web forum
- Contacting GFI Technical Support

Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit <http://kbase.gfi.com/>.

Web Forum

User to user technical support is available via the web forum. The forum can be found at: <http://forums.gfi.com/>.

Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online:** Fill out the support request form on: <http://support.gfi.com/supportrequestform.asp>. Follow the instructions on this page closely to submit your support request.
- **Phone:** To obtain the correct technical support phone number for your region please visit: <http://www.gfi.com/company/contact.htm>.

NOTE: Before you contact our Technical Support team, please have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at: <http://customers.gfi.com>.

We will answer your query within 24 hours or less, depending on your time zone.

Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit:
<http://www.gfi.com/pages/productmailing.htm>.